Review: Application Whitelisting Products p.61

Windows IT Pro

A PENTON PUBLICATION

MARCH 2011 | WINDOWSITPRO.COM | WE'RE

Sharpen Your Cloud/Mobile/ Virtualization Skills.
See details p. 20

Troubleshooting DNS in Server 2008 R2

p. 22

How DNS Works

p. 27

Michael Otey's Top 10:
Windows 7 Search Commands p. 13

Exchange Server 2010:
Mailbox Import and Export p. 31

Solve AD Replication Problems p. 37

Create Remote Sessions in PowerShell p. 42

Enterprise-Ready iSCSI:
Install and Test Storage Server 2008 R2 p. 46

Ease Deployment with SharePoint Governance p. 50

Smarter technology for a Smarter Planet:

What 3 million lines of code means to a piece of luggage.

It means Amsterdam Airport Schiphol will be able to accurately and efficiently move 70 million pieces of luggage per year—20 million more bags per year than they used to. The airport's automated baggage solution will allow Schiphol to increase their baggage handling capacity by 40%, so they can meet the growing demand placed on them as one of Europe's largest transport hubs. This system is built on IBM Rational® and Tivoli® software and runs on Power Systems.™ A smarter business is built on smarter software, systems and services.

Let's build a smarter planet. ibm.com/luggage

IBM®

A data visualization of the flow of baggage traffic at Amsterdam Airport Schiphol.

CONTENTS

Windows IT Pro
A PENTON PUBLICATION
MARCH 2011
VOLUME_17 NO_3

COVER STORY

FEATURES

INTERACT

IN EVERY ISSUE

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the InstantDoc ID text box on the home page.

COLUMNS

CONTENTS

PRODUCTS

Windows IT Pro

EDITORIAL

Editorial and Custom Strategy Director
Michele Crockett mcrockett@windowsitpro.com

Editor in Chief
Amy Eisenberg amy@windowsitpro.com

Senior Technical Director
Michael Otey motey@windowsitpro.com

Technical Director
Sean Deuby sdeuby@windowsitpro.com

Senior Technical Analyst
Paul Thurrott news@windowsitpro.com

Industry News Analyst
Jeff James jjames@windowsitpro.com

Custom Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Developer Content
Anne Grubb agrubb@windowsitpro.com

Exchange & Outlook
Brian Winstead bwinstead@windowsitpro.com

Networking, Storage, Hardware
Jason Bovberg jbovberg@windowsitpro.com

SharePoint
Caroline Marwitz cmarwitz@windowsitpro.com

SQL Server
Megan Keller mkeller@windowsitpro.com

Systems Management, Virtualization, Windows OS
Zac Wiggy zwiggy@windowsitpro.com

Editorial Web Architect
Brian Reinholz breinholz@windowsitpro.com

CONTRIBUTORS

SharePoint and Office Community Editor
Dan Holme danh@intelliem.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Joseph Edwards mje@windowsitpro.com
Kathy Ivens kivens@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com

Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Sean Deuby sdeuby@windowsitpro.com
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond 12knocksinna@gmail.com
Ed Roth eroth@windowsitpro.com
Eric B. Rux ericbrux@whshelp.com
John Savill john@savilltech.com
William Sheldon bsheldon@interknowlogy.com
Randy Franklin Smith rsmith@montereytechgroup.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Graphic Designer
Matt Wiebe matt.wiebe@penton.com

ADVERTISING SALES

Publisher
Peg Miller pmiller@windowsitpro.com

Director, International and Agency Services
Don Knox don.knox@penton.com

Business Development Director
Kerry Gates kerry.gates@penton.com

EMEA Managing Director
Irene Clapham irene.clapham@penton.com

Director of IT Strategy and Partner Alliances
Birdie J. Ghiglione birdie.ghiglione@penton.com
619-442-4064

Online Sales and Marketing Manager
Dina Baird Dina.Baird@penton.com

Key Account Director
Chrissy Ferraro christina.ferraro@penton.com
970-203-2883

Account Executives
Barbara Ritter barbara.ritter@penton.com
858-367-8058
Cass Schulz cassandra.schulz@penton.com
858-357-7649

Client Project Managers
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service service@windowsitpro.com

IT Group Audience Development Director
Marie Evans marie.evans@penton.com

Marketing Director
Sandy Lang sandy.lang@penton.com

CORPORATE

PENTON

Chief Executive Officer
Sharon Rowlands Sharon.Rowlands@penton.com

Chief Financial Officer/Executive Vice President
Nicola Allais Nicola.Allais@penton.com

TECHNOLOGY GROUP

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

WRITING FOR *WINDOWS IT PRO*
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

LIST RENTALS
Contact MeritDirect, 333 Westchester Avenue, White Plains, NY or www.meritdirect.com/penton.

REPRINTS
Diane Madzelonka, Diane.madzelonka@penton.com, 216-931-9268, 888-858-8851

THE CONVERSATION BEGINS HERE

SharePoint CONNECTIONS Coast to Coast Tour + Microsoft SharePoint BOOTCAMP

COMING TO A CITY NEAR YOU IN 2011!

DIVE INTO SHAREPOINT 2010 WITH MICROSOFT AND SHAREPOINT INDUSTRY EXPERTS.

Register now for the developer and IT pro bootcamps. **SPACE IS LIMITED!**

EARLY BIRD fee: $499

REGULAR fee: $599

REGISTER EARLY

The first 100 developers to register for the ***SharePoint Coast-to-Coast Tour*** in each city get into the hands-on *Microsoft SharePoint 2010 Development Bootcamp* for **FREE**!

A SAMPLING OF SPEAKERS

MICHAEL NOEL
CONVERGENT COMPUTING

STEVE FOX
MICROSOFT

DAN HOLME
INTELLIEM, INC.

RICHARD TAYLOR
IGOTIT TECHNICAL SERVICES

TODD BAGINSKI
FRESH TRACKS CONSULTING, LLC

MATT MCDERMOTT
ABLEBLUE

SCOT HILLIER
SCOT HILLIER TECHNICAL SOLUTIONS, LLC

ASIF REHMANI
SHAREPOINT ELEARNING.COM

CHRIS GIVENS
ARCHITECTING CONNECTED SYSTEMS

PAUL STUBBS
MICROSOFT

DARRIN BISHOP
KNOWLEDGELAKE, INC

DONOVAN FOLLETTE
MICROSOFT

ANDREW CONNELL
CRITICAL PATH TRAINING, LLC

RANDY WILLIAMS
SYNERGY CORPORATE TECHNOLOGIES

TO REGISTER: DevConnections.com/SPTour 800.438.6720

Crockett

"The pace of downsizing slowed for most industries in 2010, but the technology industry—including computers, electronics, and telecommunications—fared better than most."

More Bumps in the IT Job Recovery Road

Can IT pros finally put the Great Recession behind them?

Six months after I spoke with Rich Milgram, founder and CEO of the career site Beyond.com (InstantDoc ID 125282), I checked back in with him to see whether his prognosis for an economic recovery had changed. Milgram said last summer that recovery would come—but very slowly. In our recent conversation, he stood by his original assessment but added that the recovery will include some additional bumps along the way for IT professionals.

"The characterization of this economic recovery as jobless is not inaccurate," Milgram said. "Jobs have been the laggard. But there are certainly more opportunities than there were six months ago."

According to outplacement company Challenger, Gray & Christmas, the pace of downsizing slowed for most industries in 2010, but the technology industry—including computers, electronics, and telecommunications—fared better than most. About 46,825 technology jobs were cut in 2010, a 73 percent decrease from the 174,629 technology jobs cut in 2009. Job losses across all industries declined about 59 percent in 2010. Job losses declined sharply in the last half of 2010. As a historical note, tech job cuts represented 8.8 percent of the total job cuts in 2010. In 2001, at the height of the dot.com bust, technology job cuts represented 36 percent of job cuts.

Although the pace of job cuts is slowing, the job market still needs to catch up. Milgram said that many companies moved through a predictable cycle from slashing budgets through employee cuts to hiring lower-level IT employees.

"Now companies are in a sort of middle phase, where they're willing to spend a bit more to get employees who can more adequately do what the business requires," he said. "But companies certainly aren't hiring just for the sake of hiring. They're looking to grow—but extremely thoughtfully. There needs to be demonstrated ROI with every hire."

Companies have a relatively easy time justifying hiring IT professionals who can plan and implement hardware solutions, for example.

"If hardware specialists can demonstrate that they bring assets to the table, they can help their companies save money and produce more," Milgram said. "That's a much cleaner decision point. Talented hardware and infrastructure people provide cost benefits to companies."

Software specialists can also provide critical benefits if they can bring a combination of business value—knowledge of the company's core business processes—and technical skills. In addition, Milgram pointed to content and social media data analysis as areas with promising job prospects. According to Challenger, Gray & Christmas, mobile technology will be a strong area of growth within the technology sector, particularly with the proliferation of smart phones and tablet PCs.

"In all industries, content and social media are extremely relevant to any company," Milgram said. Content delivered through mobile applications will continue to be a big focal point for any business.

"Every company needs to think about a mobile strategy," Milgram said. "But you don't have to go out with too much—just start to test the waters by building that first app."

About 700,000 people have downloaded the Beyond.com mobile application. Although people think about email, the Internet, and mobile applications as different things, he said that IT pros looking for job opportunities should view these as simply different vantage points for content use.

Milgram reiterated his observation from six months ago that as technology becomes easier to use and manage, the IT industry will experience downward pressure on IT-related jobs and compensation.

"We'll likely continue to see people paying less for consultants now than they did in 2000," he said. "As the technology industry evolves, it's easier to keep salaries at a certain level. We might be seeing more hiring, but we won't see a big bounce-back in salaries."

Salary challenges notwithstanding, technology jobs are expected to increase not only in the next year but throughout the next decade, according to Challenger, Gray & Christmas. In particular, technologists with skills in network and data communications analysis will be in demand. Despite the decline in job cuts, finding a job will continue to be a challenge, and IT pros need to maintain a balance between specialization and general job skills.

One sure way to open more doors is to network. We at *Windows IT Pro* and our sister publications at Penton Media are producing a conference next month that will help you sharpen your skills in developing and deploying mobile applications, planning and implementing cloud computing strategies, and deploying virtualization solutions. Check it out at http://www.theconversationbeginshere.com/.

InstantDoc ID 129530

MICHELE CROCKETT (michele.crockett@penton.com) is editorial strategy director of Penton Media's IT and developer publications, including *DevProConnections, Windows IT Pro, SharePoint Pro Connections, SQL Server Magazine,* and *Connected Planet.*

James

"There are several IT products and services that can radically impact your bottom line, from virtualization and cloud computing to IT training and other programs and initiatives."

Must-Deploy IT Technologies for the Enterprise

Tough times make it more important than ever to make smart IT decisions

The economy has been battered and bruised over the past few years, and IT hasn't escaped the downturn. All of us know someone that has been impacted by layoffs, outsourcing, and other economically-driven hardships. My colleague Michele Crockett gives some excellent tips and advice on how IT pros can navigate this challenging employment climate in her column this month.

From a management perspective, surviving economic hardship isn't only about retaining the best employees. There are several IT products and services that can radically impact your bottom line. Here's a short list of some products and technologies that can save money, improve ROI, and make your IT department more agile, flexible, and responsive to business needs.

Virtualization

Just about every IT department has virtualized a few servers and achieved cost savings by reducing power consumption and the physical footprint of underutilized hardware. But server virtualization is only part of the story; desktop virtualization, application virtualization, and storage virtualization all have the potential to make IT more agile and efficient than server virtualization alone. I interviewed VMware CEO Paul Maritz a while ago (InstantDoc ID 102507), and he spoke of the potential virtualization had to make IT much more fluid, reactive, and efficient than it is today.

"[Virtualization has to become] this layer of software that truly hides all the complexity in the resource layers, whether those be hardware or software resources, and frees the application of having to know too much or being dependent upon anything else," Maritz said. "[To] really get this vision of the internal cloud to come about, anything that is tied to a physical device today has to be freed from that device. So whether it be a firewall, a router, a data scanning engine, or whatever—all those things that today are physical boxes have to transform into things that can essentially be attached to these applications and move around with the applications."

An ambitious virtualization strategy can reap rewards in terms of utility, efficiency, and cost savings, but experts warn that virtualization can open the door to expensive problems if not deployed with the right strategy and planning. "Virtualization now drives efficient IT from all angles, including data center design, platform updates, and application and infrastructure modernization, as well as traditional and new delivery models, such as infrastructure utility and cloud computing," says Philip Dawson, research vice president at Gartner. "However, virtualization does take investment; the savings are not a given."

Cloud Computing

One of the most hyped and over-used buzzwords in the IT industry is cloud computing. Our own Paul Thurrott sees cloud computing as an "ill-defined and rarely understood technology" (InstantDoc ID 126888), and many IT departments are still apprehensive about considering the technology for security, compliance, and other reasons.

But the cloud is proving to be a valuable cost-saving tool for many organizations, including the Oregon Department of Education. In 2010, they switched many of their computing needs into the cloud by switching to Google Apps for Education. All public schools in Oregon now have access to cloud-based email, website development, video conferencing, calendaring, and shareable online documents. The Oregon Department of Education estimated that "statewide cost savings for school districts utilizing Google Apps for Education is approximately $1.5 million a year for email. School districts could also realize cost savings in reduced hardware and software upgrades." (http://www.ode.state.or.us/news/announcements/announcement.aspx?=5724)

Organizations that can move services to the cloud can see some substantial cost savings, especially for complex and expensive to maintain in-house applications. In a previous column, I used the example of Penton Media's legacy in-house email newsletter tool (InstantDoc ID 129285) which was replaced by a cloud-based solution. Every organization is different, but I'm sure most IT departments have at least one or two headache applications they'd love to replace with a more efficient, less costly cloud equivalent.

IT Training

Perhaps the greatest investment any IT manager or business decision maker can make is to invest in training the IT staff they already have. Identifying what applications and services can be virtualized or outsourced to the cloud takes a unique combination of technical skill and business savvy, two traits that are always in demand by IT departments.

InstantDoc ID 129531

JEFF JAMES (jeff.james@penton.com) is industry news analyst for *Windows IT Pro*. He was previously editor in chief of Microsoft *TechNet Magazine*, was an editorial director at the LEGO Company, and has more than 15 years of experience as a technology writer and journalist.

- WSUS Code Tip
- Management Pack Explained
- VIPRE Response

LETTERS@WINDOWSITPRO.COM

WSUS Code Tip

In the December 2010 issue of *Windows IT Pro*, reader Markus Köstler suggested a modification to a script I contributed in my Reader to Reader article, "Automate the Product Update Approval Process in WSUS" (September 2010, InstantDoc ID 125613). I appreciate his constructive suggestion. I did modify the script using the searchupdates() function. However, it's not a matter of only replacing

```
$updates = $updateServer.GetUpdates()
```

with

```
foreach ($title in $ReqUpdatesFile) {
$updates = $updateServer
  .SearchUpdates($title)
 .
 .
 .
 }
```

Additional adjustments are necessary to accommodate the change. First, remove the If block that checks an update retrieved from the WSUS database against a required update (line 50 in the original script). Second, there's no need for the code block that finds missing updates (line 76); instead, just add a new variable called $InstancesCount that counts how many instances of an update are found (if any). It can be used later to count and log missing updates.

I've added the updated code to the original article. Go to www.windowsitpro.com and enter InstantDoc ID 125613.

—M. Samer Sawas

Management Pack Explained

Thank you to Pete Zerger for providing a nice dissection of a management pack ("Inside the Ops Manager Management Pack," November 2010, InstantDoc ID 126053). I've been pointing all my customers to the article. Nice work!

—Anthony Puca

VIPRE Response

Regarding Russell Smith's review of VIPRE Enterprise Premium 4.0 (January 2011, InstantDoc ID 129300), we would like to make some additional points in contrast to the reviewer's comments in the article.

VIPRE Enterprise Premium is designed to be a fast, powerful, and lightweight enterprise antivirus product, without clutter and bloat—all of which are attributes that the reviewer commented favorably on in the article. In order to optimize the performance of VIPRE and achieve these characteristics, we intentionally do not include certain features. For example, the reviewer criticized the product for its lack of a built-in NAC server (instead, VIPRE supports virtually all NAC appliances through OESIS integration). In fact, this lack of functionality is intentional. These types of additional features add bloat and bugs and are not responsive to the core demands of systems administrators, who want a high-performance antivirus product that doesn't require excessive management.

This singular focus on the core functionality requested by admins—powerful, fast, and lightweight antivirus—is the primary reason why VIPRE has become one of the most popular business antivirus products on the market, with more than 23,000 enterprise customers. Surveyed customer satisfaction for VIPRE is, in fact, higher than any other competitor on the market, including the ones outlined in this review. We respect Mr. Smith's opinions but respectfully disagree with him on their actual value or interest to the vast majority of systems administrators we communicate with on a regular basis.

—Alex Eckelberry, General Manager, GFI Software's Security Business Unit

InstantDoc ID 129528

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Thurrott

"When you combine the implications of these two rumors with Microsoft's Windows Everywhere strategy, you can see where Windows Phone, suddenly, looks like it might be living on borrowed time."

Windows 8 Rumors, Updates to Windows Phone 7, Server 2008 R2 SP1, and iPhone 4 on Verizon

While the concept of global warming is misunderstood, let's just say that New England has experienced a cooling effect this winter, surpassing annual snowfall totals a few weeks after winter started. Which is my way of saying I'm looking forward to spring, with software releases to discuss.

Windows 8 News and Rumors

At the Consumer Electronics Show (CES) in January, Microsoft revealed an interesting change coming with Windows 8, the next version of its venerable client OS. (There will be a corresponding Server version of Windows 8 too, of course.) As was expected, Microsoft will be porting Windows 8 to the ARM platform, providing a second major hardware platform, next to x86/x64, for this software. Thanks to sources at Microsoft, I'm able to report a few rumored changes coming in Windows 8.

First, to what was announced: In addition to supplying the next Windows version on traditional PCs—desktops, laptops, Tablet PCs, netbooks, and so on—Microsoft will also provide this product on so-called System on a Chip (SOC) platforms. The hardware will come from both x86/x64-based chip makers (like Intel) as well as from ARM suppliers such as NVIDIA, Qualcomm, and Texas Instruments.

Which is all very interesting, but what does it mean? First, it means using a common software platform that will run on virtually every client device type imaginable, from the smallest, low-power phone-type devices all the way up to massive, multicore gaming rigs and workstations. It means software compatibility across these devices as well, and Microsoft showed off a native Office port to ARM to drive home that point.

Second, it means that Microsoft will continue to push a Windows-centric strategy where its most popular platform can continue to thrive in a future where mainstream computing involves smaller, more mobile, connected devices. (Internally, this strategy is called "Windows Everywhere.")

More subtly, it may mean the continuation of Windows and Windows Live Division president Steven Sinofsky's longstanding policy to thwart internal projects and products that compete with the company's first-tier solutions. He did it before by killing a web-based Office competitor called NetDocs. He could be doing it again, this time to Windows Phone.

Which brings us to the rumor phase of this discussion. According to sources at the company, Microsoft is going to change the Windows UI in the next version and offer a tiered experience based on the form factor and other considerations. One of the UIs will allegedly be a tile-based UI similar to that of Windows Phone, which should answer complaints from users who hoped to see a Windows Phone-based tablet.

My sources also tell me that Windows 8 will include a new application infrastructure that bridges the gap between the proprietary, native Windows apps of today and the web. Code-named "Jupiter," this new infrastructure will support Silverlight applications that are bundled into standalone AppX packages (*.appx) and will be made available to users through a new Windows Marketplace app store.

When you combine the implications of these two rumors with Microsoft's Windows Everywhere strategy, you can see where Windows Phone, suddenly, looks like it might be living on borrowed time. We'll see whether that's the case, but some transparency from Microsoft would really be welcome at this point. Either way, we'll know more soon enough: You can expect a first beta release of Windows 8—likely a private beta—in time for the Professional Developers Conference (PDC) in September or October, followed by the final release in 2012.

Windows Phone 7 Updates in 2011

So Windows Phone may or may not be a short-lived platform, but this much is obvious: Microsoft intends to upgrade this smartphone platform several times in 2011, including a major update that should ship in time for the system's one-year anniversary in October. Unfortunately for Windows Phone fans, however, Microsoft won't be providing the equivalent of hotfixes for this system as it does on desktop and server versions of Windows. Instead it will deliver bigger updates, akin to service packs, that aggregate many fixes and build off of each other. Furthermore, each subsequent update will be a superset of the updates that came before.

So what do these updates look like? I've discovered the existence of at least two minor updates and one major update, all of which will ship in 2011. The first and most eagerly anticipated update, code-named NoDo, could arrive by the time you read this. It will consist of the widely reported copy-and-paste feature

everyone seems to be clamoring for, significant performance improvements (especially for application load times), a more granular Marketplace search, and other features and fixes.

The second major update will include CDMA support, enabling Windows Phone on the Verizon and Sprint networks in the US, as well as other changes. This will be delivered by the end of the first half of 2011.

The major update, code-named Mango, is due for "GA + 1" or one year after Windows Phone 7's initial release and could be branded with a new version number (both 7.2 and 7.5 are possible). This will include sweeping changes to the system and is, in the words of one Microsoftie who discussed the changes with me off the record, what the company wanted to ship initially but simply didn't have the time. I don't have a handle on all major feature changes, but you can expect encryption, better enterprise support, HTML 5 and Silverlight support in a new Internet Explorer version that's based on IE 9, and more.

Of course, one of the big and inevitable questions is whether Windows Phone is worth the effort. After all, credible market leaders like Google Android and Apple iPhone are already out there. In my opinion, a smartphone is essentially a two-year bet because of the way wireless carriers lock in users. And certainly Windows Phone will grow and improve over the next two years. For users, the big deal in Windows Phone is the user experience, and this is something Microsoft could easily replicate in its tiles-based UI for Windows 8. So even if Sinofsky gets his (presumed) way and Windows Phone is deemphasized for Windows, the UI, at least, could prevail.

What won't make its way across are the individual apps. But that's the beauty of Windows Phone: Thanks to its integrated services approach, apps aren't as important as they are on lesser platforms like Android and iPhone.

Update on Windows 7 and Windows Server 2008 R2 SP1

I wrote about SP1 for Windows 7 and Server 2008 R2 last year, but now that the update is finally available, it's time for a refresher. Microsoft released SP1 to manufacturing (RTM) in early February 2011, about three months later than expected, and it should be available by the time you read this. It comes in different variants for 32-bit (x86, Windows 7) and 64-bit (x64, Windows 7, Server 2008 R2) products.

On Windows 7, SP1 adds a few minor changes besides hotfixes and bug fixes, including an updated version of Remote Desktop Services, better support for third-party federation services that utilize the WS-Federation passive profile protocol, improved HDMI audio device performance, and minor XPS document fixes.

On Server 2008 R2, the picture is quite different. Here, SP1 enables two major features:

Dynamic Memory. This feature enables Hyper-V to dynamically (on the fly) distribute memory between virtual machines (VMs) based on need, without interruption of service. While Hyper-V still has some catching up to do with regards to VMware's more mature solutions, this addition closes the gap somewhat.

RemoteFX. This remote desktop technology dramatically improves the visual quality and performance of the remote user experience between a Windows 7 SP1 client and a Windows Server 2008 R2 SP1-based Hyper-V VM. It supports hardware-accelerated 3D capabilities for multimedia purposes and USB device redirection. I'll be providing a more detailed write-up about SP1 on the SuperSite for Windows (winsupersite.com).

Internet Explorer 9 RC

IE 9's improvements include the new feature set, the new hardware-accelerated, standards-based rendering, and more: The RC version adds a Tracking Protection feature in response to the US Federal Trade Commission (FTC) proposal called "Do Not Track" (which I discussed last month in "What You Need to Know About Windows 8, IE 9 Anti-Tracking, Small Business Server, and Microsoft Office Security," InstantDoc ID 129298). But it also adds some other new features.

First up is the very latest rendering engine, which is derived from the IE 9 Platform Preview releases Microsoft shipped between the September beta release and the end of 2010. This engine has been dramatically improved, and users will notice the performance difference. (Microsoft reports that the new rendering engine is over 350 percent faster than the version included in the beta.)

Next up is a refined UI. This includes nicely squared off and modern-looking UI elements such as the tabs, new address bar treatments, and other niceties.

The RC will also include a new ActiveX Filtering feature that will let users—and admins, via Group Policy—control which ActiveX controls can display. This will be integrated with the Tracking Protection feature from a UI perspective. I expect the final release of IE 9 to occur before or during the MIX11 conference, which starts April 12, 2011. See you there.

iPhone 4 on Verizon: It's Better to Wait

Finally, I'd be remiss if I didn't at least chime in on Apple's decision to sell its nearly-year-old iPhone on Verizon Wireless. Many existing iPhone customers are probably eager to jump ship from AT&T, and many Verizon customers have likely been waiting years for this day.

My advice is simple: Don't do it. Apple ships new versions of its products on a very transparent schedule, and if you migrate to iPhone 4 on Verizon now, you will be on the leading edge of a two-year contract cycle just months before the iPhone 5 (or whatever it's called) is released.

But there are other reasons to wait. The iPhone 4 is buggy hardware, with a defective antenna and proximity sensor, and there's no guarantee these will be adequately fixed until the next device arrives. The iPhone 4 is a 3G phone, and Verizon is switching to superior 4G (LTE) technology which won't work on the current device. Verizon, unlike AT&T, doesn't support simultaneous voice and data (on 3G). And Verizon's single iPhone data plan (unlimited for $30) is more expensive than the (admittedly less capable) AT&T data plans, which are $15 per month for 200MB of data and $25 for 2GB. Long story short, just wait. You can do it.

InstantDoc ID 129168

PAUL THURROTT (thurrott@windowsitpro.com) is the senior technical analyst for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Smarter technology for a Smarter Planet:

What database integration means to this blood sample.

It means doctors in Ethiopia will be able to instantly compare this blood sample to over 41,000 HIV treatment histories to help their patients receive the best treatment regimen possible. The EuResist Network is helping doctors predict patient response to various HIV treatments with over 78% accuracy—outperforming 9 out of 10 human experts in a recent study. The tool is built on an IBM analytics solution that integrates a variety of disparate databases onto a flexible IBM DB2® platform to process complex metadata more effectively than anything else on the market. A smarter organization is built on smarter software, systems and services.

Let's build a smarter planet. ibm.com/hospital

IBM®

A data visualization of 41,000 HIV case histories.

Minasi

"If you store system images as VHDs, they can serve two deployment scenarios."

Booting Windows 7 Enterprise or Ultimate from a VHD File

A little tinkering with tools from past columns delivers cool functionality

Last month, in "Creating a Bootable VHD" (InstantDoc ID 129194), I gathered all the concepts necessary to create a bootable VHD. This month, I'll again draw from past Windows Power Tools pieces to deliver a big "wax on/wax off" moment: booting a Windows 7 Enterprise or Ultimate system from a VHD. (Sorry, Windows 7 Professional, Windows Vista, and Windows XP folks—only Enterprise/Ultimate can do this.)

Two primary concepts are at the heart of boot-from-VHD. First, instead of the typical route of booting from a C volume stored on a physical drive (physical drive chopped up into volumes, volumes get names like C, and you then install an OS onto C, leaving tens of thousands of files on C), you first create not a physical hard drive but a virtual one in Microsoft's VHD format and store it as a file with a name such as image.vhd. You then mount image.vhd as a drive letter (e.g., H), install a copy of Windows onto it (in ways I've discussed in the past few months), and end up with an entire Windows boot drive—but a boot drive all neatly tied up in the one image.vhd file.

Second, you copy that VHD file onto some computer that's already running Windows and configure the already-extant copy of Windows to allow the system to alternatively boot from the VHD—not the C drive.

Why would you want to do this? If you store system images as VHDs, they can serve two deployment scenarios. In the first, you deploy desktops to people as virtual machines (VMs) running on large Hyper-V servers, and as you might know, VHD is Hyper-V's native virtual disk format. In the second, you distribute a desired desktop image to physical desktops, but instead of needing a special-purpose imaging tool such as Ghost, Clonezilla, or ImageX, your deployment tool is Windows Explorer—just drag and drop the VHD file.

So, the first part is easy: Just copy image.vhd to somewhere on the target machine. For this example, I'll assume you've copied image.vhd to a folder named C:\images. Now, all you've got to do is tell the existing copy of Windows how to allow the new alternative VHD-packaged copy to boot.

To accomplish that, you'll have to refer to two columns—"Bcdedit Basics" (InstantDoc ID 101168) and "Booting Up with Bcdedit" (InstantDoc ID 101362)—that discuss the command-line tool for controlling how Windows boots.

As those articles specify, you'll need to create a separate "OS entry" with Bcdedit before you can configure Windows Boot Manager to offer the option at boot time to boot from image.vhd (as well as booting the old way, from C). You can call the new OS entry "Boot from VHD":

```
bcdedit /copy {current} /d "Boot from VHD"
```

That gives you the OS entry's new GUID:

```
The entry was successfully copied to {61bed0dc-ddd7-11df-
   9094-70f3954a3108}.
```

Now you have to set two boot parameters in {61bed0dc-ddd7-11df-9094-70f3954a3108}: "device" and "osdevice," setting their values to "vhd=[*driveletter*:]*vhdfilespec*." Thus, as you're booting from C:\images\image.vhd, you'd type these instructions:

```
bcdedit /set {61bed0dc-ddd7-11df-9094-70f3954a3108} device
   vhd=[c:]\images\images.vhd
bcdedit /set {61bed0dc-ddd7-11df-9094-70f3954a3108} osdevice
   vhd=[c:]\images\images.vhd
```

Those are ugly commands, but you can see from the examples how to construct them: Bcdedit /set, followed by whatever GUID you got, then either *device* or *osdevice* (you need two commands, one for each), then the *vhd=…* section.

Set those up, reboot your system, and you'll see the Boot Manager and two options: *Windows 7*, which you've been using so far, and *Boot from VHD*. Choose the latter, and you're running from a VHD!

Still wondering how you might use this capability? If you need a tool to let you roll back a physical system—say, a classroom computer—as you can with a commercial product such as DeepFreeze or with Microsoft's late and lamented SteadyState, then let me suggest that you go back and read "Diskpart Takes Snapshots of Physical and Virtual Systems" (InstantDoc ID 125233), wherein I talked about how to create child/parent pairs of VHD files that could provide the snapshot capability so popular in *virtual* machines, and suggested that it might be quite useful in *physical* machines. I'll show you how to set that up, and talk about a nice (and free) tool called Wioski that implements the concept, next month.

InstantDoc ID 129377

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Administering Windows Vista Security: The Big Surprises* (Sybex).

Top 10 Free Tools for System Administrators

Audit Active Directory and file servers, detect inactive users, block USB devices, and more – for free

The following freeware tools by Windows IT Pro Community Choice Awards finalist NetWrix Corporation can save you a lot of time and make your network more efficient – at absolutely no cost. All of these tools also have advanced commercial editions with additional features, but the freeware editions will not expire and will not stop working when you urgently need them.

1. Active Directory Change Reporter (Windows IT Pro Sep'09: InstantDoc ID 102446, TechRepublic: www.tinyurl.com/6fsgrco)—This simple auditing tool keeps tabs on what's going on inside your Active Directory. The Windows IT Pro 2010 Community Choice and Editors' Best Award-winner tracks changes to users, groups, OUs, and all other types of AD objects, sending detailed daily reports with lists of changes. Download link: www.tinyurl.com/3542hnp

2. Privileged Account Manager (SC Magazine: www.tinyurl.com/68tvkq8) —This product maintains a repository of privileged user accounts (such as Administrator, root, service accounts etc) in Active Directory, servers, and other systems, providing a secure web-based portal for role-based access and automatic maintenance of shared administrative user accounts. The Privileged Account Manager can automatically generate strong passwords at specified intervals (e.g. every 30 days) and synchronize password changes on all target systems (for example, change service account password in Active Directory and update service credentials). Download link: www.tinyurl.com/46bkqvu

3. USB Blocker (Windows IT Pro Nov'09: InstantDoc ID 102860)—The increasing mobility of flash drives, MP3 players, cell phones and iPods makes the threat of data theft greater than ever, and with a couple clicks of the mouse, this aptly-named tool blocks unauthorized usage of removable media via USB ports. USB Blocker hardens end point security by preventing the spread of harmful malware and restricting the transfer of confidential information. Download link: www.tinyurl.com/65f2rtc

4. Password Expiration Notifier (Redmond Magazine Feb'09, 4sysops: www.tinyurl.com/62az8mu)—This tool automatically reminds users to change their passwords before they expire, helping keep helpdesk administrators safe from password reset calls. It works nicely for users who don't log on interactively and, thus, never receive standard password change reminders at log on time (VPN and OWA). Download link: www.tinyurl.com/5wgbn54

5. Inactive Users Tracker (MS TechNet Magazine May'08: www.tinyurl.com/4vn7gey, TechRepublic: www.tinyurl.com/5wgeeey)—This tool tracks down inactive user accounts (e.g., terminated employees) so you can easily disable them, or even remove them entirely, thus eliminating potential security holes. The tool sends reports on a regular schedule, showing what accounts have been inactive for a configurable period of time (e.g., 2 months). Download link: www.tinyurl.com/6kabf3v

6. File Server Change Reporter (4sysops.com: www.tinyurl.com/6zplvz9)—This is a must-have tool for auditing file servers and appliances. The tool detects changes made to files, folders and permissions, and tracks newly created and deleted files. The tool is useful for detecting mistakenly deleted files and it allows quick backup recovery of accidental changes. Download link: www.tinyurl.com/66v4z4r

7. Active Directory Object Restore Wizard (Windows IT Pro: www.tinyurl.com/6a9algo)—This tool can save the day if someone accidentally (or intentionally) deleted important Active Directory objects. It provides granular object-level, and even attribute-level restore capabilities that allow quick rollbacks of unwanted changes (e.g., mistakenly deleted users, modified group memberships, etc). Download link: www.tinyurl.com/68v7kdb

8. VMware Change Reporter (TechTarget/SearchVirtualDesktop: www.tinyurl.com/6fsd6xs) — If you don't know what is being changed by your colleagues in the VMware infrastructure, it's very easy to get lost and miss changes that can affect the things for which you are responsible. This tool tracks and reports configuration changes in VMware Virtual Center settings and permissions. Download link: www.tinyurl.com/6kd79fq

9. Windows Service Monitor (WindowsReference.com: www.tinyurl.com/6l44mta)—This very simple monitoring tool alerts you when some Windows service accidentally stops on one of your servers. The 2010 Windows IT Pro Community Choice and Editor's Best Award-winning tool also detects services that fail to start at boot time, which can happen, for example, with Microsoft Exchange. Download link: www.tinyurl.com/633dveq

10. Disk Space Monitor (MS TechNet Magazine Sep'09: www.tinyurl.com/6de2hdv)— Even with today's terabyte-large hard drives, server disk space tends to run out quickly and unexpectedly. This simple monitoring tool will send you daily reports regarding all servers that are running low on disk space, below the configurable threshold. Download link: www.tinyurl.com/5r8tbvh

Otey

"Although the GUI is handy, the quick access and repeatable nature of commands make them equally as important."

Windows 7 Magic Search Commands

Launch your favorite programs and utilities quickly with these keywords

In many ways, Windows's recent trend to use more commands is funny to anyone who remembers that the OS's graphical interface was always its strongest selling point: You didn't need to use commands because you could use the GUI to achieve all the things you wanted to do. Although the GUI is handy, it has become clear that the quick access and easily repeatable nature of commands make them equally as important. The Start menu search box introduced in Windows Vista and continued over to Windows 7 is one of the best examples of how Microsoft has integrated commands into the graphical Windows interface. In this column, I'll give you 10 handy commands you can type into the search box for easy access to some of the most needed Windows functions. All of these commands work under Windows 7 and most work with Vista as well. If you have your own favorite search commands, share them with me at motey@windowsitpro.com.

10 **ise—**If you're into PowerShell scripting and you're running Windows 7, Vista SP1, or Windows Server 2008, then chances are you're using the Integrated Scripting Environment (ISE). Typing *ise* in the search bar quickly starts the ISE, which lets you develop, run, and debug PowerShell scripts.

9 **displayswitch—**If you do PowerPoint presentations, the *displayswitch* command can easily become one of your best friends. Entering *displayswitch* in the search box opens the Display Switch dialog box, which lets you redirect your laptop's video output to the monitor or projector or both.

8 **snipping—**Another handy tool available in Vista, Windows 7, and Server 2008 is the Snipping Tool, which lets you quickly capture screen shots or selected parts of the screen. There's also an option to email these screen captures, which makes this handy for Help desk support. Enter *snipping* in the search box to launch the Snipping Tool.

7 **action—**You can enter the *action* command in the Start menu search box to quickly display the new Windows Action Center. The Action Center lets you diagnose system and driver problems. You can also use it to change User Account Control settings as well as Windows Update settings.

6 **network—**Using the search command of *network* launches the Windows Network Explorer. Some commands present multiple results; for example, in this case you might need to look for the result titled Network at the top of the Start menu before hitting Enter. The Network Explorer displays all the systems that are connected to your LAN. Double-clicking an icon opens a Remote Desktop Connection to the system. Right-clicking an icon opens a Windows Explorer window to the networked system.

5 **remote—**Entering *remote* in the search box is a quick shortcut for starting the Remote Desktop Connection program. Remote Desktop Connection is incredibly useful for managing remote servers or performing end-user support. By default, the program prompts you to connect with the last system that you connected to.

4 **uninstall a program—**If you want to quickly jump to Windows's *Programs and Features*, you can enter *uninstall a program* in the Start menu search box. From the *Programs and Features* window, you can uninstall previously installed applications as well as install and uninstall Windows features.

3 **word, excel, outlook, powerpoint, onenote—**The search box can be used to quickly launch any of the Microsoft Office programs. Entering *word* starts Word at a blank document; *excel* runs Excel, which starts at a blank workbook; *outlook* launches Outlook at your Mail Folders page; *powerpoint* opens a blank PowerPoint presentation; and entering *onenote* starts OneNote up at a blank notebook.

2 **msconfig—**Another handy Start menu search box command is *msconfig*. Typing *msconfig* into the search box for Vista or Windows 7 starts the System Configuration utility, which lets you control your system's startup options. Probably the most important thing here is the Startup tab, which lets you disable programs that automatically start up when the system boots but aren't really needed.

1 **resmon—**Without a doubt, my favorite command to type into the Start menu search box is *resmon*, which starts the Resource Monitor. The Resource Monitor provides a graphical dashboard showing you the processes that are running as well as the CPU utilization for all of the cores in your system. You can also monitor memory, network, and disk utilization.

InstantDoc ID 129484

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

Deuby

The Importance of Consumer Identity

The back end of consumer identity is also a type of enterprise identity

Last month, I focused on the enterprise version of cloud identity, in which the identity provider—the place that has all the user IDs, passwords, and other interesting identity information—is generally the company where you work. For 93 percent of the Fortune 1000, identity information is stored in Active Directory (AD). The driving technology in enterprise cloud identity is federation, which lets you securely extend your identity information to cloud-based services without exposing passwords over the Internet. This month, I want to give you an overview of consumer identity, which adheres to the same basic principles as federation and has similar security requirements, but is a very different configuration and has different use cases.

Why should you—the enterprise identity professional—care about consumer identity? One reason is that the back end of consumer identity is also a type of enterprise identity; after all, consumers are connecting to a business on the other end of your web browser. If your business reaches out to customers who use your company's websites, you need to have some degree of awareness or involvement in consumer identity. How do your customers authenticate to your websites? Is it easy? Is it secure?

> Take a look the next time you log on to a consumer website. Have you ever noticed how many of them are SSL-encrypted?

Another reason you should have some understanding of consumer identity is that you, too, are a consumer. And you aren't just a consumer; as a card-carrying IT pro, you're also IT support for your relatives and friends. (Why else is ThinkGeek's *No, I will not fix your computer* T-shirt perennially popular?) Not only do you need to understand the strengths and weaknesses of consumer identity security; you also need to evangelize good practices and tools to your own user community.

Today: Too Many Passwords

The biggest difference between enterprise identity and consumer identity is that in consumer identity, there's no single identity provider. In other words, there's no single authoritative identity store such as AD. Rather, every consumer service or website provides its own identity store—a bad situation in many ways. The first and most obvious repercussion is that users must remember a lot of passwords. (My current count is around 210.) Many of these passwords are also being transmitted in clear text over the Internet. Next time you log on to a consumer website, take a look: Have you noticed how many of them are SSL-encrypted? Many sites encrypt the page where users provide credit card information, but they might not encrypt the account logon page. If the logon page doesn't start with *https*, the HTTP payload packet containing the clear-text password is visible to anyone who can monitor the traffic.

Creating a strong password is obviously important. Remembering it is a pretty good idea, too. Now, repeat that for all your other websites, making sure every one is both strong and unique. It takes about three websites before password fatigue sets in, and you start repeating passwords.

Then there's the security of the identity provider to consider. It's almost impossible to know how secure your account data is with any web identity provider. The hacking of Gawker Media in December is currently the most prominent example. Gawker, which owns websites such as Gizmodo and the Gawker gossip site itself, had its company's user database hacked and its contents—more than a million users' names, email addresses, and passwords—posted to the web. One person's security breach, however, is another's research opportunity. There was a real, production user database available to analyze for security habits. One tidbit it revealed was that users' passwords for consumer sites are exactly as weak as we feared: The most common passwords for logging on to a Gawker Media site were "123456" and "password." Come on, people!

We can't be too hard on the consumer, though. It's unfair to ask the average web surfer to maintain strong, unique passwords across literally hundreds of sites, four major browser types, and probably multiple computers. I can't keep up with it, and you probably can't either.

LastPass, a browser add-on for all major browsers, is a clever solution to this problem. It captures the user ID and password you enter at a website, encrypts it locally with a one-way salted hash, and saves it to a 256-bit encrypted store on the company's servers. You have the decryption key locally on your computer, so only you can read your data. LastPass also has the ability to take care of the "don't reuse your passwords" principle by generating unique, strong (and completely unrememberable) passwords for

every website, but I haven't quite given in to that yet.

Tomorrow: Fewer, Safer Passwords

The consumer web-authentication situation isn't all doom and gloom, however. Although there isn't a single, overarching identity provider (frankly, no one wants one), there are several large, secure consumer identity providers such as eBay, Facebook, Google, Microsoft Live, PayPal, and Yahoo! The practice of re-using your existing credentials on these identity providers to log on to consumer web services (rather than creating a new set of credentials for every service) is rapidly gaining popularity. The benefits are obvious: The user no longer has to remember hundreds of passwords—just the passwords of the identity providers. There's no password to be hacked at the service provider. And the provider can get out of the identity provider business (which is secondary to its main business). Is this Single Sign-On (SSO)? Yes, but in practice, it's only SSO for the websites and services that use these technologies. The most widely adopted standards for providing this kind of consumer SSO are OpenID and OAuth.

Open ID. OpenID (openid.net) is an open standard that uses browser redirection to accomplish this sign-on process. According to its website, since its creation in 2005, more than 50,000 websites now accept OpenID for logons (which makes them *OpenID consumers*) and more than 1 billion accounts across the web have the ability to use it (because their accounts reside on *OpenID providers*). How does it work? When a web user attempts to log on to an OpenID consumer (also known as a *relying party* because they rely on identity information from the identity provider), they'll see the option to log on using an existing account at one of several OpenID providers listed on the logon page. When they click the provider's logo, they're directed to the provider's website, which asks them if they want to allow certain information (usually listed) to be provided to the website they're trying to log on to. All that's left is to click OK. For example, let's say Bob wants to log on to the stackoverflow.com website. The logon page asks, "Do you already have an account on one of these sites?" and presents him with an array of identity-provider logo buttons to choose from. (This is also known as the "NASCAR page," as it resembles a wall of corporate logos you might find on a NASCAR race car.) He chooses Google and is redirected to a Google Accounts page, where he's asked whether he wants to allow sharing of his Google email account with Stackoverflow. (This consent step happens only once.) After clicking Allow, he's sent back to Stackoverflow, where he's now authenticated with no more action on his part. Pretty easy.

OAuth. OAuth (oauth.net) isn't strictly about authentication, but it can do it. OAuth is currently being used mainly for web service authorization. However, two websites you might have heard of—Facebook and Twitter—use OAuth for authentication. Facebook uses it for Facebook Connect, which lets you use your Facebook account to log on to other websites, and Twitter requires it for all applications that wish to access Twitter data. Therefore, even though OAuth isn't widely adopted for authentication, it's heavily used. In the future, OAuth is expected to become very popular for authentication on mobile devices because its authentication process doesn't require a browser.

Given a choice of identity providers, I'm more comfortable with some than with others.

That said, given a choice of identity providers, I'm more comfortable with some than with others. On one hand, every place where you can log on to Google is encrypted, and so are all Gmail transactions. Facebook's default logon, on the other hand, is unencrypted. Did you know there's an SSL sign-in page for Facebook? Just add an "s" to the "http" in the Facebook URL. Facebook doesn't advertise this fact, however. Without SSL encryption, all your Facebook transactions are visible on the network, which allows exploits such as Firesheep to capture and use your session cookies to hijack your account. And Facebook's somewhat *laissez faire* approach to privacy isn't encouraging.

Then there's the consideration of identity quality. An identity is created at an identity provider, but how "real" is it? Is a real person behind it, with real information, or has it been generated by a spambot? If this is something you're concerned about as a service provider, a financial services identity provider such as Verisign or PayPal jumps to the top of your preferred list because they have more stringent verification requirements.

The Future: Your Identity Scattered in the Cloud?

Looking forward, cloud identity gurus are looking at the use case in which some identity providers have many parts of your online identity (but no one has all of it), and your full online consumer digital identity is an aggregate of identity bits from many identity providers. Google might contain your email address, PayPal your bank account number, Facebook your friends and your birthday (if you aren't careful), and Windows Live your gaming information and Kinect visual profile. How can you securely provide just the right amount of these different sets of identity data to, for example, a mobile device? And how do you easily control access to the data? This step involves federation between the identity providers themselves.

The web is moving toward fewer passwords, using standards such as OpenID and OAuth. Until then, utilities like LastPass can programmatically handle the multiple-password problem for you. If you work for a consumer-facing service, you should be evangelizing OpenID or OAuth to eliminate the overhead and vulnerability of maintaining your own identity store. And you should encourage your user community to log on with their existing identity providers when they can, try SSL logons if they can't and it's available, and use LastPass to increase personal security.

InstantDoc ID 129422

SEAN DEUBY (sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine*, and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

READER TO READER

A Fast Way to Find EFS Folders and Files

Encrypting File System (EFS) has been available since NTFS 3.0 and Windows 2000. With it, you can encrypt individual files, encrypt an entire folder, or configure a folder so that all the files that users save in it will be encrypted.

Harry Verge

In most cases, it's extremely important to find every encrypted folder and file that might reside on a computer before you do something to that computer. For example, suppose you have a server that you want to promote to a domain controller (DC). Before promoting it, you need to make sure that all encrypted folders and files have been found and dealt with. The same holds true if you're demoting a DC. (If you didn't, the Microsoft article "Unable to Recover Encrypted Files After the Domain Controller Is Demoted" at support.microsoft.com/kb/276239 can help you through this predicament.)

Another example of when you want to be completely sure you have no EFS folders or files on a computer is when you're installing some third-party encryption software. Not surprisingly, some of this software doesn't play nice with already encrypted folders or files. But what is surprising is that there are vendors out there that don't even do a preliminary check for EFS folders or files before allowing the software install to merrily proceed.

You should also know about all EFS folders and files before a file migration, before swapping out hard drives, before removing a computer from a domain, and before deleting or reseeding user profiles. A good rule of thumb is to know about all EFS folders and files before performing any invasive operation that could potentially leave the encrypted data inaccessible. By knowing about the existence (or non-existence) of EFS folders and files, you can gauge how to proceed. If you're sure no EFS folders or files exist, you can rule out needing to decrypt or export certificates and private keys before proceeding.

There are various tools available to find encrypted folders and files. I'll discuss several of them, including a VBScript script I created. But before I do, let's make sure there's at least one EFS folder and one EFS file on your computer so you can try them out.

Figure 1: Encrypting the test file

Creating an EFS Folder and File

On your test computer, create an empty folder named EFS-Test at C:\Program Files\Common. Mark the newly created folder for EFS encryption by doing the following: right-click it, choose Properties, click the Advanced button, select the *Encrypt contents to secure data* check box, and click OK.

Next, create a test file named EFS-Test.txt at C:\Program Files. Mark it for EFS encryption by following the same general steps just described, except this time select the *Encrypt the file only* check box (see Figure 1) because the file is in an unencrypted folder.

Now that you have at least one EFS folder and one EFS file on your C drive, let's look at how you can find them. Specifically, I'll discuss how to use the built-in Windows Search functionality, the EFSinfo tool, the Cipher utility, and the EFS-Find.vbs script.

Using Search

If you have lots of time on your hands or are looking for extra pain in your life, one tool you could use to find encrypted folders and files is Windows's Search functionality. By searching for *.*, you can get a list of every single folder and file on your hard drive. You then need to look through all the results for any folder or file that's highlighted in green (assuming you haven't changed the default color for EFS folders and files). I don't recommend this approach, but I wanted to mention it because you can find encrypted folders and files this way in a pinch.

Using EFSinfo

A slightly better way to find EFS folders and files is to use Microsoft's EFSinfo command-line tool. You can find it in the \Support\Tools

A Decade of Making the Connection

For over 10 years, DevConnections and Microsoft have collaborated to bring you the premiere developer and IT events in our industry.

HIGHLIGHTS OF CONNECTIONS 2010 SHOWS INCLUDE:

FRED J. STUDER, General Manager, Information Worker Business Group Lead, US Business Marketing Operations, Microsoft, & **SHAUN PIERCE**, General Manager, Lync Server Division, Microsoft, celebrate the release of Microsoft Lync

BOB MUGLIA, President, Server and Tools Business, Microsoft, launches Visual Studio 2010

SCOTT GUTHRIE, Corporate Vice President, .NET Developer Platform, Microsoft, launch of Silverlight 4

JOE BELIFORE, Corporate Vice President, Windows Phone Program Management, Microsoft, announces Windows Phone 7 to the developer community.

Many surprises happened including attendees of our Windows Phone 7 pre-conference workshop at our November 2010 DevConnections show received a free Windows Phone 7.

Collaboration between DevConnections and Microsoft continues, bringing great insight for developers like you into how to use the newest technologies. What will you and your team see at DevConnections in 2011? You'll need to sign up and be there to find out!

Our unique format of Microsoft Day sessions and third-party sessions let DevConnections attendees get the inside word from Microsoft followed by the practical realities of using Microsoft technologies in the field at clients around the world.

Don't Miss the exciting 2011 Connections Events: Many surprises are still under wraps!

- Train with 150+ Microsoft architects and world-renowned speakers delivering 290+ in-depth sessions.
- Keep your competitive edge by staying on top of the latest technology and visit sessions in the co-located events at no extra charge!
- Connect with colleagues and build a valuable network of peers
- Workshops help you dive into key areas including: SharePoint collaboration, hands-on jumpstart on Exchange Server 2010 SP1, hands-on exploration of Microsoft Lync Server 2010, professional development in SharePoint 2010, SharePoint Business Connectivity Services (BCS), integrating SharePoint 2010 with Exchange 2010 and Lync 2010, and organizing information in SharePoint 2010

JOIN THE CONVERSATION

Schedule at a Glance

SUNDAY, MARCH 27, 2011	
7:30 am	Registration Opens
9:00am - 4:00 pm	Pre-conference Workshops
6:30pm - 8:30pm	Keynotes
MONDAY, MARCH 28, 2011	
7:00 am - 5:00 pm	Conference Registration
7:30 am - 8:30 am	Continental Breakfast
8:30 am - 10:00 am	Keynote
10:00 am - 11:00 am	Expo Hall Open
11:00 am - 12:15 pm	Conference Sessions
12:15 pm - 1:45 pm	Lunch
1:45 pm - 6:15 pm	Conference Sessions
6:15 pm - 7:45 pm	Expo Hall Reception
8:00 pm - 9:30 pm	Special Evening Events
TUESDAY, MARCH 29, 2011	
7:00 am - 5:00 pm	Conference Registration
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 9:15 am	Keynote
10:15 am - 1:00 pm	Conference Sessions
1:00 pm - 2:30 pm	Lunch
2:30 pm - 5:15 pm	Conference Sessions
5:30 pm - 6:30 pm	Vendor Sessions
WEDNESDAY, MARCH 30, 2011	
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 1:00 pm	Conference Sessions
10:30 am - 2:30 pm	Expo Hall
1:00 pm - 2:30 pm	Lunch
2:15 pm	Cruise Raffle
2:30 pm - 3:30 pm	Conference Sessions
4:00 pm - 4:30 pm	Closing Session & Prize Drawing
THURSDAY, MARCH 31, 2011	
9:00 am - 4:00 pm	Post-conference Workshops

CRUISE GIVEAWAY

Enter to WIN!

Enter the contest in the Expo Hall to

WIN a 1 week Caribbean Cruise for two!

You must be present in the Expo Hall at the time of the drawing to win.

Cruise does not include travel or hotel. Value is $2500.

CONFERENCE AND EXPO INCLUDES:

Exchange and Windows Connections registration includes a one-year (12 issues) print subscription to *Windows IT Pro* magazine for Exchange and Windows conference attendees only. Current subscribers will have an additional 12-months added to their subscription. Subscriptions outside of the United States will be served in digital; $12.50 of the funds will be allocated toward a subscription to *Windows IT Pro* ($49.95 value)

SharePoint Connections registration includes a print subscription (4 issues: March, June, Sept, Nov) to *SharePointProConnections* magazine for SharePoint and Windows conference attendees only. Current subscribers will have an additional one year (4 issues) added to their subscription. Subscriptions outside of the United States will be served in digital.

Your Conference registration includes:

- Three Continental Breakfasts
- Three Lunches
- Reception
- Conference T-Shirt and Bag
- Proceedings Resource CD ... and more

EMS01: HOW MICROSOFT IT IMPLEMENTED MICROSOFT EXCHANGE SERVER 2010

EMS02: USING MICROSOFT EXCHANGE SERVER 2010 TO ACHIEVE RICH COEXISTENCE WITH EXCHANGE ONLINE

EMS03: WHAT'S NEW IN ARCHIVING, RETENTION, AND DISCOVERY IN MICROSOFT EXCHANGE SERVER 2010 SP1

EMS04: WHAT'S NEW IN OWA, MOBILITY AND CALENDARING IN MICROSOFT EXCHANGE SERVER 2010 SP1

EMS05: MICROSOFT® LYNC™ SERVER 2010: TRANSFORMING THE WAY PEOPLE COMMUNICATE

EMS06: MICROSOFT® LYNC™ SERVER 2010: WHAT'S NEW IN DEVICES

EMS07: BUILDING COMMUNICATIONS ENABLED BUSINESS PROCESSES WITH MICROSOFT® LYNC™ SERVER 2010

EMS08: MICROSOFT® LYNC™ SERVER 2010 INTEROPERABILITY: VOICE, VIDEO, CONFERENCING, IM, AND PRESENCE

EXC01: THE EXCHANGE SERVER STORE DEMYSTIFIED

PETER O'DOWD

So just how does the Exchange Store work? Understanding this is critical to improve your chances of recovery from a disaster. Find out how, with topics including: Log files and database signatures; correct use of eseutil; checkpoint depth; missing log files; how the extensible storage engine actually works, improvements with Exchange 2010. What is in the header of a database, why do I care? Peter has travelled the globe teaching both inside and outside of Microsoft on this topic. If you want to understand the store then this is your session.

EXC02: TELEPHONY DEMYSTIFIED FOR EXCHANGE ADMINS (PART 1)

PETER O'DOWD

Need to understand telephony concepts quickly? Don't have days to spend researching things you probably won't need to know? Let Peter bring you up to speed in this first of his two killer sessions for demystifying telephony concepts. Learn just what you need about business phone systems and PBXs, circuit switching, trunk lines, dial plans, hunt groups to be able to plan and implement your Unified Messaging solution. This sessions is a must for any Exchange administrator who is about to dive into Unified Messaging with Exchange. Session is also relevant if you are considering Microsoft Lync!

EXC03: TELEPHONY DEMYSTIFIED FOR EXCHANGE ADMINS (PART 2)

PETER O'DOWD

In this second of two killer sessions on demystifying telephony concepts you will start to apply your new understanding of telephony to how it works with Exchange Server 2010 UM. Avoid spending days researching things you probably won't need to know. Let Peter bring you up to speed with call flows between PBXs and Exchange UM servers. Learn about VOIP Gateways and when you need them, Outlook Voice Access call flows, the SIP protocol and how it works, call answering rules and auto attendant. This second session is a must for any Exchange administrator who is about to dive into Unified Messaging with Exchange.

EXC04: CLIENT ACCESS SERVER 2010–FINALLY SERVING ALL CLIENTS!

KEVIN LAAHS

The CAS role plays an even bigger role in your Exchange 2010 environments than it does in Exchange 2007. Whilst it still supports the likes of OWA, ActiveSync, and Exchange Web Services, there are some fundamental architectural changes that will change the way you architect your Exchange environments. In this session we take a look at the major new functions that the CAS supports such as the Exchange Control Panel and "Mapi-On-The-Middle Tier" (for Outlook clients) as well as all the exciting end user features that are delivered by the likes of OWA and ActiveSync (even to Firefox and Safari browsers).

EXC05: EXCHANGE WEB SERVICES –FOR EVERYONE!

KEVIN LAAHS

PowerShell is often considered within the realm of IT Administrators, whereas Web Services is firmly in the developer camp–and usually, never the twain shall meet! But now the combination of PowerShell and Exchange Web Services can be harnessed by end users to build and run scripts to manage mailbox data from desktop machines. This session shows IT Administrators, developers and end users alike how friendly Web Services can be, and how you can easily leverage them to automate many operations in your Exchange environment.

EXC06: EXCHANGE, SHAREPOINT AND OFFICE–BETTER TOGETHER?

KEVIN LAAHS

What integration points exist between SharePoint 2010, Office 2010 and Exchange 2010? Does the combination of these three flagship products (and other such as OCS) bring any new opportunities for my overall environment? And what about the existing integration points that were there in the 2007 suite of products? Are they still available? In this session we'LL answer the numerous questions in this abstract! The session first looks at how Outlook 2010 lights up when connected to Exchange 2010 followed by a trip around many of the integration points between various products in the overall ecosystem (such as, searching SharePoint content from Windows, viewing user pictures from multiple locations and overlaying SharePoint and Exchange calendars).

EXC07: THE RPC CLIENT ACCESS ARRAY: THE MISSING PIECE OF EXCHANGE AVAILABILITY

DEVIN L. GANGER

Exchange 2010's Database Availability Group functionality has received a lot of press and hype (and deservedly so) for enabling better, easier HA scenarios. There's a missing piece, however: the RPC Client Access Array. This session, drawn from real-world examples, explains what the RPC Client Access Array object is (and what it isn't), when you need it, and how to deploy it. Devin will also examine how deploying RPC Client Access Arrays affects the clients, load balancers, reverse proxies, and other parts of your Exchange organization. We recommend you take this session in conjunction with the session: Load Balancing for Exchange Deployments.

EXC08: LOAD BALANCING YOUR EXCHANGE DEPLOYMENT

DEVIN L. GANGER

When it comes to highly available Exchange deployments, a lot of attention is focused on the Mailbox role. As the CAS role in Exchange 2007 and Exchange 2010 takes over more of the client connections, load balancing incoming connections at the CAS and Hub Transport becomes more important to successful Exchange deployments. This session, drawn from real-world examples, examines the requirements, caveats, and best practices available for designing appropriate load balancing solutions for Exchange 2007 and 2010 deployments. It compares Windows Network Load Balancing, software load balancers, and hardware load balancers. We recommend you take this session in conjunction with the session: The RPC Client Access Array: The Missing Piece of Exchange Availability.

EXC09: WAN OPTIMIZATION FOR EXCHANGE

DEVIN L. GANGER

WAN optimizers provide on-the-fly bandwidth reduction for a variety of applications: mainly websites and file services. However, Exchange MAPI-RPC client sessions may also benefit from these devices. This session, drawn from real-world exam-

ples, explains how current WAN optimizer offerings work with MAPI, both client-to-server and server-to-server, and helps give you information to assess what kind of bandwidth savings you might see in your environment. How does SMB signing affect your optimization? Can optimization be extended to mobile clients? Can optimization help with the replication of multiple DAG copies into a secondary site? Devin will examine these topics and provide clear answers to help you determine if WAN optimization is right for you.

EXC10: EXCHANGE 2010 HIGH AVAILABILITY WITHOUT THE HIGH COST

JIM MCBEE

In older versions of Exchange, achieving high availability required more servers, third-party products and/or additional storage technologies. Clustering in Exchange Server 2010 has evolved into database availability groups (DAGs). Unlike previous versions where availability and databases are tied to a specific servers, with DAGs a database can be active on any server within the availability group and each database can be made active on any server within the group. This session will cover using Exchange Server 2010 in a small or medium sized business (under 1,000 users) where you want to achieve high availability. Topics include database availability groups, Client Access arrays, and providing high availability for the message transport when using two server DAGs.

EXC11: MIGRATING TO EXCHANGE 2010 FROM EXCHANGE 2003

JIM MCBEE

This session will cover the practical aspects of migrating from Exchange Server 2003 to Exchange 2010 including meeting the necessary prerequisites, interoperability, and potential showstoppers. Topics include factors to evaluate before migrating, the steps necessary to prepare your organization, mail routing, web client redirection, moving public folder content, and moving mailbox data.

EXC12: MAKING GOOD IT BUSINESS DECISIONS WHILE CLOUD PROOFING YOUR CAREER

JIM MCBEE

Outsourcing IT services to the cloud is a topic that is frequently on everyone's mind, but often not properly discussed. Depending on whose marketing material you read, EVERYONE should outsource their e-mail to a hosted provider. In many cases, outsourcing makes good business sense as long as you consider all of the corporate, political, or legal restrictions. But where does that leave the on-premises admin? Can you take effective steps to cloud-proof your job? What kinds of things should you be doing to build a protective umbrella of your own value to help you if the clouds come to your office? This session examines the business economics of outsourcing e-mail services to the cloud while offering some practical tips to help you weather cloudy times.

EXC13: FOREFRONT TMG CLIENT ACCESS PUBLICATION AND EDGE TRANSPORT INTEGRATION

MIKE CROWLEY

During this session, Mike will cover two aspects of Exchange and TMG integration. In the beginning, he'll discuss the installation procedures and configuration requirements of TMG and Edge's residence on the same server. In the second half, he'll demonstrate the steps of publishing Exchange client access through TMG.

EXC14: INFORMATION RIGHTS MANAGEMENT EXPLORED

MIKE CROWLEY

During this session, we will discuss and then demo IRM and S/MIME, the infrastructure requirements for both, the pros and cons, and configuration.

EXC15: OFFICE 365

MIKE CROWLEY

This session will cover capabilities, migration, and administration of the Office 365 and Live@EDU environments. It will include demonstrations and best practices.

EXC16: HIGH-AVAILABILITY WITH THE OTHER ROLES: HUB TRANSPORT, CLIENT ACCESS, AND UNIFIED MESSAGING

MICHAEL B. SMITH

Most high availability discussions focusing on Exchange revolve around the mailbox server. However, there are other significant roles that need to be considered: Edge, HT, CAS, and UM. In this session we will cover the basic concepts behind HA and the details associated with configuring the Edge, HT, CAS, and UM roles for HA.

EXC17: DUMPSTER AND LITIGATION HOLD–DUMPSTER 2.0 VS. DUMPSTER 1.0

MICHAEL B. SMITH

Exchange 2010 introduces a new dumpster-Dumpster 2.0. In this session, we will discuss when Dumpster 2.0 takes effect and how it differs in operation with SingleItemRecovery enabled (or not), with Retention Hold, with Discovery Searches, and otherwise. We will deep-dive into how this information is stored in the Exchange ESE database.

EXC18: CONFIGURATION AND USAGE OF RETENTION POLICIES IN EXCHANGE 2010 SP1

MICHAEL B. SMITH

Exchange 2010 introduced Retention Policies to replace Managed Folders. In RTM, Retention Policies were not very useful. In this session, we

will discuss how to provide functionality approximately equivalent to that provided by Managed Folders and what additional features that Retention Policies provide to the business and end-users.

We will deep-dive into how these items are stored in Active Directory and what functionality is lost and can be controlled by the Exchange administrator.

EXC19: EXCHANGE 2010 DEPLOYMENT AND MIGRATION BEST PRACTICES

KIERAN MCCORRY

Exchange 2010 is yet another version of Exchange. Its architecture and topology is similar to that introduced with Exchange 2007, but there are some important changes and restrictions on interoperability that any organization in the early stages of planning a move to Exchange 2010 should be aware of. This session will give an overview of the best practices for Exchange 2010 deployment and focus on the interoperability and migration aspects from previous versions of Exchange.

EXC20: EXCHANGE 2010 SP1

KIERAN MCCORRY

There's nothing like waiting for the first service pack before looking in earnest at a new product deployment. Exchange 2010 Service Pack 1 brings a host of improvements and enhancements to the core platform. In this session, we'll see what comes with the update and why it makes sense to think about deploying Exchange now that SP1 is here.

EXC21: EXCHANGE 2010 INFORMATION PROTECTION AND RETENTION

KIERAN MCCORRY

Exchange 2010 brings with it the most comprehensive set of Exchange features yet from Microsoft to help you safeguard and protect your data and where it goes in your Exchange organization. This new version has sophisticated rules for controlling information flows within the organization and taking actions when certain events occur. In addition, Exchange 2010 has a completely revamped model for information retention and archiving by means of the Online Archive. This session will describe those new features and explain what it means for you as a system administrator and your users as information workers.

EXC22: BRINGING IT ALL TOGETHER: INTEGRATING EXCHANGE, LYNC, AND SHAREPOINT

PAUL CHARBENEAU

Now that you have Exchange, Lync, and SharePoint, how do you get the most out of those investments by getting them to work together? This session will show you how to integrate services from Exchange, SharePoint, and Lync Server so that common data and user experience is provided across your Unified Communications framework. Same picture in Communicator, Outlook, and SharePoint? Sure. Want to IM from OWA? No problem. Paul Charbeneau will walk through these features and will also demo Office Web App, PowerPoint broadcasting, and co-authoring with SharePoint.

EXC23: EXTENDING ON-PREMISE EXCHANGE INTO THE CLOUD WITH OFFICE 365

TOM PHILIPS

As you know, Exchange is taking a big step into the cloud. It offers companies an opportunity to move some or all mailboxes off-premise. This can be an appealing option for distributed organizations with many users in one location and several users spread around the globe. In this session, Tom Phillips, who has been working with Microsoft on Office 365 federation for several months, will discuss and demo how you can split your users between an on-premise Exchange Server 2010 server and off-premise Office 365 Exchange.

EXC24: CAN LYNC SERVER 2010 REPLACE YOUR PBX?

THOMAS FOREMAN

Have you been waiting to replace your PBX with a full VoIP solution, but were unsure of Office Communications Server? Are you curious about Lync Server 2010 and its new Enterprise Voice features? Come to this information-packed session that will review all of the features of Lync Server 2010 that qualify it as a full VoIP solution that can replace your PBX. Microsoft has worked hard at being able to make the claim that Lync Server is a full PBX solution, come see what new features allow Microsoft to make this claim. Gain important knowledge and see detailed demonstrations that show the features that make Lync Server 2010 a full PBX solution such as the Call Park feature, Voice Resiliency at the data center and at branch offices, Malicious Call Tracing, Call Admission Control, Media Bypass, New Devices, Enhanced 911, and more. Come see how Lync Server 2010 is so much more than just a PBX solution and then take this information back to begin your deployment.

CHECK WEB SITE AS WE CONTINUE TO ADD MORE SESSIONS, SPEAKERS AND MAKE UPDATES

WWW.WINCONNECTIONS.COM

POWERSHELL–THE BASICS AND MORE

ADVANCED WINDOWS 7 DEPLOYMENT SCENARIOS USING THE MDT 2010 – PART 1

ADVANCED WINDOWS 7 DEPLOYMENT SCENARIOS USING THE MDT 2010 – PART 2

INTRODUCTION TO APPLICATION VIRTUALIZATION (APP-V)

INTRODUCTION TO MICROSOFT ENTERPRISE DESKTOP VIRTUALIZATION (MED-V)

BRINGING TRADITIONAL DESKTOP COMPUTING, MOBILITY AND CLOUD COMPUTING TOGETHER

USING ACT 5.6

WINDOWS XP MODE IN WINDOWS 7

USING A USB DRIVE TO DEPLOY WINDOWS 7 WITH THE MDT 2010

DIRECT ACCESS: THE DEATH OF THE VPN

TOP 10 REASONS TO UPGRADE TO WINDOWS SERVER 2008 R2

HYPER-V: SECURING YOUR VIRTUALIZATION ENVIRONMENT

WIN01: DON JONES'S 75-MINUTE POWERSHELL CRASH COURSE

DON JONES

If you can run "Ping," then you can start using PowerShell to automate a huge number of administrative tasks. In this concentrated, information-packed session you'll learn the key secrets of making PowerShell easier to use and more effective, and you'll see common administrative tasks automated right before your eyes. Create users in AD, retrieve management information from remote computers, calculate last startup time for servers, and much more. You'll also learn the tricks to teaching yourself new PowerShell techniques, opening the door to automating Exchange, System Center, SharePoint, IIS, and much more.

WIN02: DON JONES'S SECRETS OF CLIENT AND SERVER REMOTE CONTROL WITH WINDOWS POWERSHELL

DON JONES

Windows has finally caught the command-line wave, and PowerShell is your new, command-line "remote desktop!" Learn the secrets of how PowerShell remote control enables you to securely and efficiently control both server and client computers. You'll learn how to use the one-to-one "remote shell" option as well as the super-efficient one-to-many technique that controls multiple remote computers in parallel. PowerShell expert Don Jones details the underlying protocol and configuration settings, giving you all the details as well as the best practices you need.

WIN03: DON JONES'S ADVANCED WINDOWS POWERSHELL: ERROR HANDLING, DEBUGGING, "SCRIPT CMDLETS," AND MORE

DON JONES

Take PowerShell further by turning simple commands into powerful, reusable tools that you can distribute to other administrators! Learn how PowerShell error-handling works to add error logging and logic to your tools, and learn the tricks that experts use to debug PowerShell scripts faster and more efficiently. PowerShell expert Don Jones also provides all sample scripts, and a complete shell transcript, for download after the conference, giving you ready-to-use templates and tools to use as a starting point back home.

WIN04: VDI-IN-A-BOX: MICROSOFT DESKTOP VIRTUALIZATION FOR SMALLER SCENARIOS AND BUSINESSES

GREG SHIELDS

Today's talk about VDI centers around deploying hundreds or thousands of desktops. But sometimes you just want access for a few people and a few applications. Or, you just can't afford big-budget solutions. Have you tried Microsoft Hyper-V and RDS? Combining these two tools, a sufficiently-powerful server, and the information in this session, you'll quickly build a single-server VDI solution for just those small needs. Join RDS MVP Greg Shields for a look at the very small in VDI. He'll show you how to get started on the most micro of budgets, and send you home with the exact click-by-click to begin hosting your own virtual desktops.

WIN05: PREPARING SOFTWARE FOR DEPLOYMENT WITH A WINDOWS 7 UPGRADE

GREG SHIELDS

Application guru Greg Shields hates walking around the office, DVDs in hand. He hates clicking Next, Next, Finish to install software. He also hates dealing with applications that are directly installed into his Windows 7 deployment images. That's why he taught himself software packaging, and automated software installation for a company of thousands. Join Greg in this session to learn his tricks for repackaging software. Then you too can automatically deploy applications with your Windows 7 deployments.

WIN06: AUTOMATICALLY DEPLOYING WINDOWS 7 WITHOUT THE MICROSOFT ALPHABET SOUP

GREG SHIELDS

Greg Shields may be most known for his books, magazine articles, and conference sessions, but he started his career deploying thousands of computers from a basement of a building with no windows. His passion for deploying Windows is fed by his desire to automate everything. You can do that with Microsoft's free tools. But while the tools are fantastic, their alphabet soup of acronyms is confusing and their documentation isn't much better. Learn Greg's seven simple steps in 75 minutes or less, and leave with a framework for automating everything in Windows 7 deployment.

WIN07: MICROSOFT OPALIS 101: YOUR SECRET IT PRO AUTOMATION BUDDY, ENGINE, AND SECRET WEAPON

JEREMY MOSKOWITZ

By the time you read this abstract the tool Microsoft recently bought called Opalis might have a new name. It might be called something like "Microsoft Automation Engine." Heck, the original name of this product was the super-cool name "Opalis Robot" so you know it's gotta do some kick-butt stuff. What does it do? It's your code-free automation engine to push the dozens to hundreds of buttons from system to system, so you don't have to. When an alert or condition happens, you want to know about it, of course, but you also want the problem to just go away. If you can dream of the "automatically fix it" scenario, Opalis is there to be your invisible (and automatic) arms and fingers. In this session, you'll learn about the moving parts of Opalis as well as some key scenarios where you can use this tool right away.

WIN08: MICROSOFT AND 3RD-PARTY GPO TOOLS YOU HAVE NEVER HEARD OF (AND SOME YOU HAVE)

JEREMY MOSKOWITZ

It's now more important to "do more with less." And if you're an Active Directory administrator, you're also a Group Policy administrator. And that means you need to do more with what you've got. The good news is, there are a gaggle of free, low cost, and pay tools to help round out your Group Policy experiences. Some tools are in the box, downloadable from Microsoft or available with a license. Some tools we'll explore are third-party tools. Together, these tools can help you troubleshoot, lock down your desktops, make your applications more secure, manage what you've got more efficiently, and be a better administrator. In this session, you'll walk away with a huge list of

applications you can experiment with today to see if they're a good fit for your environment and see if you can really "do more with less."

WIN09: TOTAL WORKSTATION LOCKDOWN: YOUR ACTION PLAN

JEREMY MOSKOWITZ

Total workstation lockdown isn't for every machine in your organization, but some machines require it. It's usually those "public walk up" machines that we need to manage a little bit differently; the machines that are in the cafeterias, the lobby and the library. The more we think about it, these kinds of machines are everywhere in our organization—inviting attack and ruining our day. Who knows what crazy things people are doing on these machines—visiting strange websites and installing evil software. The good news is that Microsoft has a slew of solutions to help you with this very specific problem. And it doesn't mean you need to turn the thumbscrews and go from 0 - 100% lockdown either. Microsoft has a variety of technologies you can choose (and mix and match) to make sure your workstations are locked down only as much as they need to be. In this session, Group Policy MVP Jeremy Moskowitz will demonstrate a myriad of ways to make your public desktops more secure. You will also learn about some non-Microsoft tools to help enhance your control of this notoriously difficult situation.

WIN10: VMWARE ESX BEST PRACTICES: NOTES FROM THE FIELD

ALAN SUGANO

Over the years of installing ESX, we have developed a list of best practices when implementing ESX. These include ESX Host Selection, Storage Groups, SAN Design, Storage Planning, Thin versus Thick provisioning, vCenter Server, Backup, Cloning Virtual Machines, Security, Virtual Machine OS Selection, and Physical to Virtual (PtoV) Conversions. All of these practices were developed as a result of real-world implementations of ESX. Find out how to avoid potential pitfalls when implementing ESX and ensure a stable, secure and fast virtualization infrastructure.

WIN11: THE CLOUD CONTROVERSY: AN IN-THE-TRENCHES VIEW OF YOUR COMPANY'S PLACE IN THE CLOUD

ALAN SUGANO

Cloud computing is a hot, controversial topic. Some experts see it as a major paradigm shift, while others think it's an incredibly bad idea. We'll examine what the major cloud vendors have to offer and companies where cloud computing is a good fit. Going forward I foresee many companies adopting a hybrid approach to place items in the cloud when it makes sense, but still retaining their core infrastructure on-site. We'll examine some of the challenges facing migration to the cloud including WAN connections, security, regulatory requirements, and network configuration.

WIN12: PASS A PAYMENT CARD INDUSTRY (PCI) COMPLIANCE SCAN (AND WHY YOU'D WANT TO EVEN IF YOU DON'T HAVE TO)

ALAN SUGANO

If your company accepts credit cards, there's a good chance you need to be PCI compliant. So you do the right thing and sign up for your first PCI scan and the results are longer than War and Peace. Where do you start? This session will give you tips to help your company become PCI compliant and what you should do to remain compliant. What's that—your company isn't concerned about PCI compliance? You still need to attend this session, because it highlights security practices that are relevant to every company, no matter what their security needs.

WIN13: CONDUCTING A FORENSIC COMPUTER INVESTIGATION FOR IT STAFF

MIKE DANSEGLIO

Computer crime has been on the rise for decades. There are many situations where an incident occurs that doesn't break the law but is still cause for concern, such as corporate policy violations, information mishandling, or internal system compromise. Many companies are forming their own internal investigative units to address these situations. In this session, we'll examine what kinds of investigations can be handled internally, when and how to engage law enforcement, how to best prepare for incidents, and the best practices to use. We will also focus on building your computer investigation toolkit including the tools you should have and how you should use them.

WIN14: NETWORK SNIFFING FOR IT PROS, NOT HACKERS

MIKE DANSEGLIO

The IT pro has a great variety of network monitoring tools and techniques available today. But many believe these are the tools of evildoers or spies. This session dispels the myth by showing how to use tools like Wireshark to capture, analyze, and troubleshoot common network problems during everyday operations. You'll see a number of examples of network problems including network storms and server failures as well as more expected issues like nefarious intruders and audio and video streams causing network failures.

WIN15: THE NETWORK FILES, CASE #53: DIAGNOSING DISEASES OF DNS

MARK MINASI

Network troubleshooters soon learn that the first place to look when the network stops working is DNS... and soon after that, they learn that the in-the-box DNS troubleshooting tool, nslookup, is a pretty weak answer—but this session remedies that with a clear, step-by-step set of diagnostic approaches and prescriptions for DNS ills of all stripes. Give your troubled DNS queries a thorough workup with Network Monitor, and find out why those dynamic updates aren't happening. Get the scoop on the dreaded "eDNS flu," an ailment endemic to Server 2008 and 2008 R2 boxes. Take your DNS system's pulse with DNSLint. Take a sample of your DNS output with a close examination of your logs, and more. Attend this session and you'll soon be known as "Doctor DNS!"

WIN16: BEND R2'S ACTIVE DIRECTORY TO YOUR WILL

MARK MINASI

Most of us who have to manage an AD sometimes run into a problem like "I need to disable all accounts that haven't logged on in the past 60 days," only to find that Active Directory Users and Computers doesn't seem to be able to help much there. (It can, actually but you'd have to put on your diving helmet and sink many fathoms into LDAP query-land to get the job done.) So you wonder, "What to do here?" and start talking yourself into solving the problem by hand, click by click. You KNOW a few days of writing a VBScript or two might solve the problem, but that's an awful lot of work so, again, what to do? Microsoft's given us the answer in their 76 shiny new Active Directory-related PowerShell commands. With a bit of practice, you can glue two or three PowerShell commands into a powerful one-liner that can do what used to take three days and 150 lines of VBScript... even if you've never written a line of code. Join command-line techofreak Mark Minasi in a quick, clear guide to the PowerShell commands you need—and how to make them work together. Every attendee will leave prepared to create their first "one-liner!"

WIN17: TEN (OR MORE) THINGS YOU PROBABLY DON'T KNOW ABOUT WINDOWS SERVER 2008 R2

MARK MINASI

Okay, so maybe you've read about or even played around with Windows Server 2008 R2. You know a bit about Active Directory's PowerShell cmdlets, DirectAccess, BranchCache and the new backup program. It's all great stuff, but... did you know that R2's the first print server whose spooler service WON'T crash just because a print driver failed? Or that R2's DHCP server service has a cool new MAC filter feature, combined with helpful new support for split scopes? Well, that's just the start. Ever needed to resize a VHD? R2's got command-line support for that, as well as a whole new kind of built-in SMB cache. And of course you know that R2 shores up your system's security by blocking those scary old 1980s LM-type logons—but did you know

that R2's got the tool that you need to smoke out and stomp those persistent early 90s NTLM logons? Join server geek Mark Minasi in a fast-paced review of all of the R2 features that haven't really gotten the attention that he thinks that they ought to, complete with demos and step-by-step instructions to try them out in your own network. Hey, what would be crazier than paying for a new server operating system and not squeezing all of the juice out of it?

WIN18: GOING, GOING, GONE? VIRTUALIZING YOUR ACTIVE DIRECTORY FOREST

SEAN DEUBY

Is your company going through a server consolidation project using virtualization? Has the project team come to you and asked you to prove why they shouldn't virtualize the entire Active Directory? Does this make you uneasy? It should! There are ways to safely virtualize your AD—but you shouldn't do it all, and if you don't do it right you could endanger your entire forest. Learn from Sean how to safely virtualize and manage your domain controllers, with the best practices from the Microsoft Directory Services Team.

WIN19: THE BEST FREE TOOLS FOR WINDOWS DESKTOP ADMINISTRATION

GREG SHIELDS

IT professionals are a unique group. We're tasked with the ultimate responsibility of our business' critical applications and data, but we're rarely given a budget to do so. Heck, many of us aren't even allowed to see the budget. As a result, we're forced to either beg for tools or find them for free on the Internet. Cheapskate IT pro Greg Shields has been collecting the very best free tools for over ten years, and wants to share those in his quiver with you! In this must-see session, Greg highlights the very best no cost Windows tools—some you've used, many you've never seen. Join this session and leave Windows Connections with a brand new toolset for solving the daily tasks in desktop administration.

WIN20: ACTIVE DIRECTORY FEDERATION SERVICES (ADFS)—WHY YOU SHOULD CARE AND WHAT YOU SHOULD KNOW

LAURA HUNTER

Active Directory Federation Services (ADFS) 2.0 is designed to meet the growing demand for a single sign-on solution that crosses organization, application and platform boundaries. In this session you will learn about the need for ADFS in a multitude of scenarios, followed by a description of the features and capabilities of the newest release of ADFS 2.0, as well as best practices from Microsoft's internal ADFS team on how to deploy a secure and highly available ADFS 2.0 deployment.

WIN21: INSTALLING ACTIVE DIRECTORY FEDERATION SERVICES (ADFS) 2.0

SEAN DEUBY

The rise of cloud computing has finally given federation technology a real purpose: safely extending your company's Active Directory identities to cloud service providers, instead of creating and managing separate accounts for every provider you use. How do you take the first steps in becoming federationally proficient? Directory expert and MVP Sean Deuby will show you how to install and configure Active Directory Federation Service 2.0 so you can start gaining hands-on experience with this technology.

WIN22: HOW MSIT DEPLOYED ACTIVE DIRECTORY FOR WINDOWS SERVER 2008 AND R2

LAURA HUNTER

Recycle Bin and RODCs and beta builds, oh my! In this session, come and hear true stories from Microsoft's internal Active Directory team on how we tested and deployed Windows Server 2008 and R2 across a large multi-forest environment. We'll include an overview of some of the new Active Directory features in 2008 & R2 that an upgrade brings to the table, as well as tried-and-true methods of planning and implementing an upgrade in a large, complex environment...along with some hints, tricks, and "gotchas" that we faced along the way.

WIN23: BETTER WINDOWS IMAGING: THE VIRTUAL HARD DISK (VHD) FORMAT

RHONDA LAYFIELD

Creating images to deploy to 10 or 10,000 machines has never been easier. Microsoft has supported the .wim image format for quite a while now but there is a new image format with even better features called "virtual hard disk" (.vhd) images. The old .wim image format forced you to create an image of every partition on your hard disk and when it came time to deploy you had to apply multiple images to your clients. With virtual hard disk images (.vhd) you can create one image that contains multiple partitions reducing the amount of time it takes to create and deploy your Windows images. There are some new tools to help you with .vhd images like "Disk to VHD". Disk to VHD allows you to take an existing installation and turn it into a virtual hard disk image that can be deployed to many machines. Or you can create a .vhd image from scratch in under an hour but you really need to understand where the pain points are. And last but not least, find out which Microsoft deployment technologies support deploying .vhd images and which do not.

WIN24: DEPLOYING WINDOWS IMAGES THE SAFE, SECURE WAY

RHONDA LAYFIELD

Deploying Windows images involves lots of different user account credentials. Credentials for joining a machine to a domain, creating computer objects and don't forget about that local administrator account's password on the newly deployed machines. Find out where and how these credentials are stored in the Microsoft Tools and how one tool differs from another. This session will help you learn about securely deploying Windows images using Windows System Image Manager (WSIM), Microsoft Deployment Toolkit 2010 Update 1 (MDT 2010 U1), Windows Deployment Service (WDS) and System Center Configuration Manager 2007 (ConfigMgr).

CHECK WEB SITE AS WE CONTINUE TO ADD MORE SESSIONS, SPEAKERS AND MAKE UPDATES

WWW.WINCONNECTIONS.COM

DEVELOPMENT TRACK

HDEV01: DEVELOPERS DEEP DIVE INTO SHAREPOINT SECURITY
TED PATTISON

SharePoint 2010 introduces a new claims-based security model that will impact the way that companies design, implement and enforce security with their SharePoint sites. This session explains the fundamental concepts of a claims-based model and shows how the new claim-based model makes it possible to use new types of security principals such as Active Directory distribution lists and SharePoint Server Audiences as first class security objects which can be used to securely configure access to securable objects such as sites, lists, items and documents. The session will walk through developing a custom claims-provider with Visual Studio 2010 which will effectively demonstrate the flexibility of how we define the people and groups from whom you need to configure access.

HDEV02: SHAREPOINT DATA ACCESS SHOOTOUT
TED PATTISON

When developing for SharePoint 2010, there are many different ways to access items in a list. When writing server-side code you can use the SPQuery class or the SPSiteDataQuery class. You can optionally use the new LINQ to SharePoint Support which enables you to write LINQ query statements against SharePoint lists. When writing client-side code in JavaScript or Silverlight you can use the CamlQuery class provided by the new client-side object model. You also have the option of using the new REST-based Web service built into SharePoint Foundation or creating your own custom Web service. This means there are different ways for you to query and update items. This session examines each of these techniques in depth and reveals their strengths and weaknesses in terms of performance, productivity and maintainability.

HDEV03: ADVANCED CONTROL AND WEB PART DEVELOPMENT
TED PATTISON

Web Parts aren't the only type that's useful in SharePoint development. This session will begin with a quick primer on creating custom controls for SharePoint sites and demonstrate several examples including development with user controls and delegate controls. The session also examines the SharePoint Web Part architecture where you will learn the role of the Web Part Manager and the Web Part Gallery. The session demonstrates several different styles for Web Part rending including using an XSLT transform to generate HTML output. Along the way, this session will discuss using persistent properties, creating custom editor parts as well as taking advantage of Web Part verbs, Web Part connections and using asynchronous processing when retrieving data from across the network.

HDEV04: RECORDS MANAGEMENT IMPROVEMENTS IN SHAREPOINT 2010
JOHN HOLLIDAY

SharePoint 2010 introduces many new content management features that can be applied to build both document and records management solutions. In this session, we'll examine these features in detail and explore ways to apply them to solve traditional records management problems such as creating hierarchical file plans, using metadata to drive content routing and making e-Discovery more accessible for records managers and end users. During the session, we'll also explore the new in-place records management features that make it easier to manage compliance details for individual documents, and we'll take a closer look at the improved Records Center site to see how it combines all of the new content management features to simplify the creation of a locked-down records vault.

HDEV05: SHAREPOINT 2010 RECORDS MANAGEMENT DEVELOPMENT
JOHN HOLLIDAY

The SharePoint 2010 Content Organizer introduces a new approach to content routing, providing end users with greater flexibility to setup custom routing rules without custom coding. This is great for most situations, but there are still times when standard rule definitions are not enough, particularly when building custom ECM/RM solutions. In this session, you'll learn how to configure a Records Repository programmatically so that it understands and processes incoming document types consistently across the farm. We'll also develop custom information policies and work with the Content Organizer entirely in code to generate and process rules, and extend it to handle real-world scenarios, such as routing content to external RM systems.

HDEV06: CONTENT TYPE DISCOVERY USING DEPENDENCY STRUCTURE MATRIX ANALYSIS
JOHN HOLLIDAY

Content types are the cornerstone of every Enterprise Content Management solution built on the SharePoint platform. However, finding a consistent and repeatable methodology for identifying the appropriate content types for a given solution remains a challenge for most organizations. Dependency Structure Matrix (DSM) analysis has been around for more than 30 years, and has been applied to everything from process modeling to Software Architecture. This session will explore the use of DSMs to identify content types by deriving functional groups based on interdependencies that exist between content elements flowing into and out of business processes.

HDEV07: BUILDING CUSTOM APPLICATIONS (MASHUPS) ON THE SHAREPOINT PLATFORM
TODD BAGINSKI

Custom applications which combine components from several different systems, services, and data sources are more commonplace in today's world than ever before, not to mention they are usually the most fun to build! This session shows how to combine Business Connectivity Services, the SharePoint client object model, SharePoint Search, Silverlight, Bing Maps, Twitter, the Digital Assets Library (Images & Videos), SharePoint list data, and even SharePoint's new rating functionality to create a "mashup" application that provides a wide variety of functionality. In this session, you will learn how to combine all of these components to create eye-catching applications built on the SharePoint framework.

HDEV08: BUSINESS CONNECTIVITY SERVICES (BCS) DEVELOPMENT PATTERNS
TODD BAGINSKI

In this session, you will learn how you can apply repeatable patterns with Business Connectivity Services to work with external data in SharePoint 2010. This session will discuss the different authentication, authorization, and data access options used to connect to external data sources and when each is most appropriate. This session will also discuss modeling complex types and entity associations in a Business Data Connectivity (BDC) model, explain how filtering and throttling works in the BDC runtime, and map common external data scenarios to different data modeling approaches. This session will also demonstrate the different approaches you can use to interact with external data and when each one is appropriate. After attending this session, you will understand when BCS should be used and how to implement it properly.

HDEV09: INTEGRATING WINDOWS 7 MOBILE APPLICATIONS WITH SHAREPOINT SITES
TODD BAGINSKI

How many times have you heard someone say, "There's an app for that?" Have you ever wanted to create your own mobile application? How about one that integrates with SharePoint? In this session, you will learn how Windows Mobile 7 makes it easy for .NET and Silverlight developers to make the transition and develop applications for mobile devices. You will learn how to develop a Windows 7 Mobile application which integrates with SharePoint websites and other services.

HDEV10: UPGRADING WEB PARTS FOR USE ON SHAREPOINT 2010
MAURICE PRATHER

Web Parts have been around for three generations. We'll talk about all the different ways Web Part code can be upgraded. We'll discuss how to best move your Web Parts from where they are today to where you want them tomorrow.

HDEV11: BUILDING CLAIMS-AWARE APPLICATIONS AND CONTROLS
MAURICE PRATHER

What exactly are claims? In this session, we'll quickly cover the fundamentals of claims authentication. Then we'll dive into details needed to leverage claims within your applications.

HDEV12: SHAREPOINT GUIDANCE: DEVELOPING APPLICATIONS–FOUNDATION AND EXECUTION
ROBERT L. BOGUE

In this action-packed session you'll get a guided tour around the foundation and execution portions of the Microsoft patterns & practices SharePoint Guidance. As a member of the team that built the guidance, Robert will talk through the guidance both from the perspective of the documentation generated as well as the reference implementations and core library. Expect to leave wanting to spend more time mining the value of the SharePoint Guidance.

HDEV13: ENHANCING THE SHAREPOINT SOCIAL EXPERIENCE WITH THE SHAREPOINT 2010 SOCIAL API
MATT MCDERMOTT

This session focuses on the developer interfaces for the Social Computing API and Web services for SharePoint 2010. Social Computing with SharePoint involves creating people-aware applications that take advantage of User Profiles, Social Data, and Personalization built into SharePoint. This session will demonstrate development techniques for:

- Using SharePoint 2010 User Profiles
- Working with the SharePoint User Profile and Social Data Web Services
- Taking action on User Profile Changes
- Using Social Data in Custom Applications Outside the Firewall

HDEV14: EXPLOITING THE "HIDDEN GEMS" OF THE SHAREPOINT SOCIAL API
MATT MCDERMOTT

This session focuses on two new, and often overlooked, features of the SharePoint User Profile Application that can be used to enhance the end user experience and drive user adoption of SharePoint personal features. This developer-oriented approach demonstrates techniques to leverage the social API and the User Profile Service to create applications that provide business value.

This session will demonstrate development techniques for:

- Consuming SharePoint Social Data
- Creating Organizational Profiles for Official and Ad-Hoc Teams
- Create BDC Connections to Increase Findability of Corporate Data
- Classify Users to Enhance the User Profile Experience for the Organization

HDEV15: ECM FROM A DEVELOPER'S PERSPECTIVE
PAUL SWIDER

Developers can use the SharePoint ECM programming model to extend the functionality of the new ECM features and create custom document management solutions. In addition, SharePoint 2010 introduces the Managed Metadata store as the enterprise tool for managing taxonomy. In this session you will learn how to add rich ECM functionality to your SharePoint sites using members of the taxonomy and document management object model. At the end of the session you will understand the pros and cons of each namespace.

HDEV16: BUILDING APPLICATIONS WITH THE CLIENT OBJECT MODELS
SCOT HILLIER

One of the top requests from customers for SharePoint 2010 was that it include more Web service access to the API. Microsoft responded by providing a client-side object model that makes client programming as seamless as server-side programming. In this session, we will cover the fundamentals of the three different client object models: .NET, Silverlight, and JavaScript. Attendees will learn to use the client object models to create solutions that can run within SharePoint or stand-alone. Attendees will leave the session with a strong understanding of the new client object model and how to utilize it in their programming tasks.

HDEV17: ADVANCED SEARCH-BASED SOLUTIONS IN SHAREPOINT 2010
SCOT HILLIER

Search-based solutions are applications that use a search page as the primary interface. Solutions such as image searching or travel searching in Bing are good examples of search-based solutions. SharePoint 2010 offers developers new ways to extend search and create search-based solutions. In this session, attendees will learn to create advanced search-based solutions such as task management and navigation. Attendees will leave with many new ideas for using search to deliver end-user productivity.

HDEV18: DEVELOPING RICH CLIENT SOLUTIONS WITH BUSINESS CONNECTIVITY SERVICES
SCOT HILLIER

Creating External Lists with Business Connectivity Services is all the rage, but what about the client side? In this session, we'll cover the development techniques for creating client-side BCS solutions. We'll start with declarative solutions designed to customize the BCS experience. Then we'll move on to creating custom Office 2010 add-ins for BCS. Finally, we'll show how to create Windows applications that use BCS data. Attendees will exit with lots of new ideas for creating BCS solutions that run on the client.

ADMIN TRACK

HITP01: WISH I'D HAVE KNOWN THAT SOONER! SHAREPOINT INSANITY DEMYSTIFIED
DAN HOLME

After years of helping organizations around the world to deploy and implement SharePoint, Dan Holme has found that there are certain pain points

that almost everyone encounters. Some are confusing concepts. Some are bad decisions driven by Microsoft's UI and documentation. Some are due to unnecessarily complex terminology. And some because there are things that SharePoint should do, but can't. In this session, Dan will share the most common and problematic scenarios, and their solutions, with the goal of saving you pain, time, and money. Think of this session as "Lessons Learned," "Best Practices," or "From the Field" on steroids. Whether you're new to SharePoint or a seasoned veteran, in this grab-bag session there will be treasures for you!

HITP02: SHAREPOINT 2010 DEPLOYMENT DEMOFEST

BEN CURRY

Come get a first look at proven SharePoint Server 2010 deployment Best Practices. This session is full of real-world lessons learned, tips, and tricks learned from the field. Ben will give you a LIVE guided tour of a multi-server farm deployment. Learn the basics for creating and managing Web and Service applications, scaling services, and selecting basic server farm topologies for most implementations.

HITP03: ARCHITECTING A SHAREPOINT SERVER 2010 FARM

BEN CURRY

So, you are ready to install or upgrade to SharePoint Server 2010 but don't know where to start? All of the options and endless combinations of service application topologies can be overwhelming. This session provides a thoughtful approach to designing your SharePoint Server 2010 server farm and gives you confidence that you are heading in the right direction. You'll learn about the service application architecture, common design decisions for scaling service applications, Web application considerations, and how your logical architecture will affect the physical farm topology.

Attendee Key Takeaways–Understand SharePoint Server 2010 farm topologies at the 200 level and have a game plan for designing your farm when you get back to the office. Understand the basics of service application architecture, how many servers you'll need, what the hardware requirements are, and how your logical Web application design and user load will impact the physical architecture.

HITP04: ARCHITECTURE BEHIND THE SOCIAL COMPUTING PLATFORM IN SHAREPOINT 2010

BEN CURRY

This session will show you how to plan, design, and implement the UPA to provide the platform for social computing in SharePoint Server 2010. There are many misconceptions about how the service application, along with associated service instances and databases, is implemented. Only when this foundation is correctly configured will you realize the full potential of social computing. This session will include the service application architecture, synchronization with Active Directory, managing user profiles, designing and implementing My Sites, and managing user metadata such as ratings.

HITP05: DESIGNING GOVERNANCE: HOW INFORMATION MANAGEMENT AND SECURITY MUST DRIVE YOUR DESIGN

DAN HOLME

You've read the white papers, you've "Binged" governance, but how, exactly, do you design a SharePoint implementation that will support governance, security, and information management? Join SharePoint MVP and consultant Dan Holme for a practical, nuts-and-bolts look at the close relationship between your information management requirements and SharePoint's manageability controls, and the demands that relationship places on your design and infrastructure. This session is focused on architecting a logical design of SharePoint that effectively supports your information management requirements and governance plan–the "technical" side of governance. You will learn how to align your governance requirements with SharePoint farms, Web applications, and site collections. You'll discover why some third-party applications are a "design poison pill" and what SharePoint 2010 offers to greatly improve the deployment of a governable design. Gain a deeper understanding of the intricacies and challenges of designing the logical structure of SharePoint, and take away practical, blueprint-like guidance to what a governed SharePoint implementation might look like in your enterprise.

HITP06: A PRACTICAL JUMP START TO ADMINISTERING SHAREPOINT WITH WINDOWS POWERSHELL

DAN HOLME

Windows PowerShell is the preferred tool for administering and automating SharePoint outside of Central Administration and only with PowerShell can you perform scripted configuration and certain tasks such as granular restore. So if you've been holding back on learning PowerShell, the time has come to tackle it. Join SharePoint MVP Dan Holme for a very practical, super-clear PowerShell jump start. You'll learn that you don't need to be a scripting guru to use and understand PowerShell and you'll learn how easy it is to manage SharePoint with PowerShell.

HITP07: INFORMATION ARCHITECTURE AND THE MANAGED METADATA SERVICE: A TO Z

DAN HOLME

Join SharePoint MVP Dan Holme for a down-and-dirty, deep examination of the configuration and management of the Managed Metadata Service, and what the MMS does to support your enterprise information architecture. You'll explore every nook and cranny of this powerful service application, and see how to provide both centrally managed taxonomy and user-driven folksonomy for enterprise tags. You'll also explore content type syndication and best-practice guidance for topologies to support your information architecture.

HITP08: WINDOWS POWERSHELL FOR SHAREPOINT ADMINISTRATORS AND DEVELOPERS

DON JONES

Welcome to the future! Microsoft's promise to make administration available through PowerShell continues to come true, most recently in SharePoint Server 2010. Now all you need to do is figure out what to best make use of the shell, whether you're trying to automate administrative tasks, or want to use the shell as a ".NET Immediate Window." PowerShell guru Don Jones introduces you to the shell's key concepts, including under-the-hood functionality like pipeline binding, to make you effective without writing a line of script. You'll learn the patterns that govern SharePoint's PowerShell cmdlets, and you'll learn to wrap them into your own reusable, parameterized tools. You'll see how to directly access .NET Framework classes from the shell, and you'll learn how developers can incorporate the shell (and the functionality it provides) from within your own .NET code.

HITP09: SHAREPOINT SERVICE ARCHITECTURE DRILL-DOWN

JOEL OLESON

The most important decisions you'll make in a SharePoint deployment relate to the decisions around the service application architectural decisions. There are nearly 20 service applications and figuring them out and configuring them can be a very daunting task. A common deployment mistake is to simply install all services not knowing what is needed. We'll take look at these services and how they should be configured for best performance and high availability.

HITP10: UPGRADING TO SHAREPOINT 2010

JOEL OLESON

We'll start with the In-Place Upgrade and Database attach upgrade methods, but the real focus is on the strategy behind the various hybrid upgrade methods. We'll walk through an upgrade decision tree and arm you with the best strategies behind how best to provide uptime and the best user expe-

rience and achieving IT goals at the same time.

HITP11: SHAREPOINT SEARCH CHALLENGES AND TRICKS
MATTHEW MCDERMOTT

Many organizations struggle with SharePoint search configuration when it falls outside simple document search. This session presents strategies for handling special search scenarios like large files, images and video. This session also presents techniques for metadata tagging of files that are outside of the control of the search team. The tips and techniques are presented as patterns that can be used in many different search situations.

- Search configuration overview
- Large file search configuration
- Image metadata tagging and search
- Image search result configuration
- Tagging and searching files you don't control

HITP12: BUILDING THE PERFECT SHAREPOINT 2010 FARM: REAL-WORLD BEST PRACTICES FROM THE FIELD
MICHAEL NOEL

SharePoint 2010 is nearly a year old, with improvements in scalability, enterprise search, and administration. Best practices from SharePoint 2007 are no longer relevant, and new guidance has emerged from the last year worth of SharePoint deployments. New features such as SharePoint FAST Search capabilities can have a significant effect on how an environment is architected. In addition, the popularity of server virtualization technologies have created new design options for SharePoint administrators, allowing for new and unique high availability and provisioning options. This session goes right to the heart of the matter, providing for physical and virtual architecture guidelines and specific configuration settings that can immediately be used to construct SharePoint 2010 environments that can be used to replace existing SharePoint 2007 farms. Architectural specifics are based on best practices obtained from existing SharePoint 2010 environments of multiple sizes and performance metrics gathered from both physical and virtual SQL Server and SharePoint environments will help you to build the "perfect" SharePoint 2010 farm for your organization.

- View real-world SharePoint 2010 deployment models for environments of multiple sizes, including virtualized SharePoint farms
- Gain access to specific design criteria for sizing a SharePoint farm and providing for high availability for all components
- Get information to be able to build the "perfect" highly available, high performance and scalable SharePoint 2010 environment that will stand the test of time

HITP13: ARCHITECTING A FAULT TOLERANT AND HIGH PERFORMANCE SHAREPOINT 2010 FARM
MICHAEL NOEL

Significant architectural changes have been made between SharePoint 2007 and SharePoint 2010, including a complete removal of the infamous Shared Services Provider and the ability to have redundant indexing functionality in a farm. In addition, the number of databases in a single farm has increased significantly and Microsoft has overhauled the authentication model used by SharePoint. All of this translates to some significant architectural changes between SharePoint 2007 farm architecture and SharePoint 2010 farm architecture, changing the paradigm for SharePoint infrastructure architects. This session focuses on outlining how the changes in SharePoint 2010 architecture allow for new design scenarios, and how you can design a new fault tolerant and high performance SharePoint 2010 environment to migrate your existing SharePoint 2007 content into.

- Learn how the significant architectural changes between SharePoint 2007 and SharePoint 2010 change how to design a SharePoint farm.
- Examine best practice farm architecture and real-world SharePoint design models.
- Learn best practice advice for how to prepare to re-architect a SharePoint 2007 environment for an eventual migration to SharePoint 2010.

HITP14: PLANNING EXTRANET ENVIRONMENTS WITH SHAREPOINT 2010
MICHAEL NOEL

Organizations planning for extranet access to SharePoint 2010 or faced with providing access to an intranet from multiple internal authentication platforms often find it challenging to properly architect SharePoint for extranets, to isolate content, and to manage identities across disparate systems. The complexity involved in understanding how to isolate content from a security perspective but still provide for a collaborative space for end users is complex, and if not done correctly can lead to security breaches and confusion. This session focuses on understanding the various extranet models for SharePoint 2010 and providing real-world guidance on how to implement them. Covered are extranet content models and extranet authentication options, including advanced options using tools such as Microsoft's Forefront Identity Manager (FIM) 2010 to centralize identity management to SharePoint 2010 farms, allowing for better control, automatic account provisioning, and synchronization of profile information across multiple SharePoint authentication providers.

- Review extranet design options with SharePoint 2010
- Understand the need for identity management across SharePoint farms
- Examine real-world deployment guidance and architecture for SharePoint environments using multiple authentication providers

HITP15: CLAIMING TO GET FORMS-BASED AUTHENTICATION
ROBERT L. BOGUE

Not everyone has an account in your active directory. Sometimes you need to work with people outside the organization. Whether you're working with customers, vendors or partners, you'll need to figure out how to implement forms authentication–and how to manage the users. Password expiration, forgotten passwords, and the need to delegate the permission to create accounts are all real issues you need to be able to deal with. In this session, we'll walk you through the setup of a farm for forms-based authentication (via claims) and implement some of the key account management features you'll need (with the help of some reusable code).

HITP16: PROTECT YOUR SHAREPOINT FARM FROM THE EVIL DEVELOPERS
ROBERT L. BOGUE

Whether you believe your developers are evil or just under informed, SharePoint 2010 has a set of tools for you to use to protect yourself from a developer breaking your entire farm. In this session, you'll get an IT pro's introduction to the SharePoint Sandbox and how it can help you including code isolation and execution quotas. You'll also learn about protection from long running queries, and how you can put the pieces together to keep your farm running no matter what the developers throw at it.

NO CODE SOLUTIONS TRACK

HNCS01: MANAGE YOUR EXTERNAL DATA USING BUSINESS CONNECTIVITY SERVICES ... WITHOUT CODE
ASIF REHMANI

The Business Connectivity Services (BCS) is an evolution of the concept of Business Data Catalog (BDC) that was introduced in SharePoint 2007 to get access to your line of business data. In addition to consuming your data, BCS lets you also write back data to your external systems. SharePoint Designer 2010 is used to define your connection properties by creating External Content Types (ECT) without the need for programming! In this session, you see how you can surface this data using external lists, metadata in SharePoint lists and also your Outlook application to create robust business solutions.

HNCS02: USE DATA VIEWS TO GET TO YOUR DATA — BOTH INSIDE AND OUTSIDE OF SHAREPOINT

ASIF REHMANI

You can use SharePoint Designer to make connections to and present data from internal and external data sources such as SharePoint lists, libraries, xml files, databases and Web services. The focus of this session is on exposing the data to the user using the XSLT Web Parts. These Web Parts can be manipulated in a variety of ways to present the information to the end user. In this session, you'll see how the list view and data view tools can be used to reformat the presentation of the data using conditional formatting, pre-formatted styles, xPath expressions and more.

HNCS03: AUTOMATING BUSINESS PROCESSES USING INFOPATH 2010 FORMS WITH INTEGRATED SHAREPOINT DESIGNER 2010 WORKFLOWS

ASIF REHMANI

Forms and Workflows are essential to business processes. Companies usually rely on programmers to create the forms and workflows using code. Not any more! If you have access to Microsoft InfoPath 2010 and Microsoft SharePoint Designer 2010, you can create powerful data-driven form solutions on your SharePoint sites. InfoPath gives you the ability to pull data from databases and lists, and create forms with data validation and conditional formatting. SharePoint Designer's workflows let you then design powerful multi-step workflows centered around the form collected data. In this session, you see how to design a robust form using InfoPath and then design a workflow using SharePoint Designer to route this form appropriately.

HNCS04: USING INFOPATH 2010 AND SHAREPOINT DESIGNER 2010 TO MANAGE SHAREPOINT LIST FORMS

ASIF REHMANI

SharePoint Designer has been a great tool to customize SharePoint list forms for a long time. Now in SharePoint 2010, you can use InfoPath 2010 to customize the forms as well. What's the difference? Why should you use one tool over the other for this purpose? This session shows how each functionality works and explores the pros and cons of using each method to customize your SharePoint list forms.

HNCS05: PERFORMANCEPOINT SERVICES 2010: BUILDING A DASHBOARD IN 60 MINUTES OR LESS

DARRIN BISHOP

The title says it all. Creating dashboards are now simple thanks to PerformancePoint Services 2010. As a matter of fact there is no code involved. This session will show you how to create and publish a dashboard in 60 minutes or less. We will step-by-step create all the components needed to surface your data inside a PerformancePoint dashboard. Creating and publishing dashboards is a quick and easy way to make you the hero of the company.

HNCS06: UNDERSTANDING POWERPIVOT AND WHAT IT BRINGS TO THE TABLE

MAURICE PRATHER

PowerPivot is the newest member of the Microsoft BI stack. We'll examine what it is and how it can be used within the corporate environment.

HNCS07: SOLUTIONS WITHOUT SEMICOLONS — THE IT PROS GUIDE TO SOLUTION CREATION

ROBERT L. BOGUE

Many organizations are struggling to get the support they need. The IT pro is being asked to help create solutions for business units. The Office System including SharePoint, Visio, InfoPath, Word, and SharePoint Designer are tools that the IT professional can use to create solutions that don't require a single semicolon. In this very practical session, we'll create a few solutions that every IT pro can create that will look like you stayed up all night to learn a new (foreign) language.

HNCS08: USING OUTLOOK AND THE SHAREPOINT WORKSPACE WITH SHAREPOINT 2010

SCOT HILLIER

SharePoint 2010 provides powerful ways to use data offline through Outlook 2010 and the SharePoint Workspace. In this session, you'll learn how to synchronize sites, lists, and libraries with Outlook and the SharePoint Workspace. You'll learn how data is installed and managed on the client so that you can understand the proper way to work with offline data. You'll learn limitations and workarounds associated with offline data including conflict resolution and collaborative document creation. Attendees will exit this session with a complete understanding of how offline data is synchronized, managed, and utilized in Office clients.

SHAREPOINT COMMUNITY TRACK

HSCM01: SHAREPOINT BRANDING: CREATING A SUCCESSFUL BRANDING PROJECT MAP

CATHY DEW

Successful branding projects start out with a detailed plan to determine the user needs from a content perspective and the branding needs. By learning what can be created for branding SharePoint Server 2010, and evaluating the components (master pages, CSS, page layouts, themes) you can create a project map. In this session I will also cover what the initial considerations needed to allow for a phased approach to implementation and leave room for future growth.

HSCM02: CREATING CONSISTENCY IN USER INTERFACE DESIGN WITH SHAREPOINT 2010

CATHY DEW

Once a determination has been made to create a custom branded SharePoint 2010 site, you will need to keep in mind all the pieces/parts that need to be created. You must also consider other components that must be decided in regards to the levels, types of sites and functionality of the sites and how the branding will function across all of these pieces. This session will focus on the best practices surrounding master pages, alternate CSS and page layouts for an Intranet site including what to use where and how far you should push the boundaries of customization.

HSCM03: DON'T JUST MIGRATE—TRANSFORM YOUR SHAREPOINT ENVIRONMENT

CHRISTIAN BUCKLEY

Migration is not just a technical activity (provision a new system, attach and move databases), but should be a much more thoughtful and planned activity. This session will help attendees understand the difficulties surrounding migration, and the ample opportunities to transform their data–building a new system that meets their environment vision. We will discuss fundamentals of capacity planning, the overall migration schedule, how to involve end users in the process, understanding the as-is and to-be system views, outline strategies for taxonomy and metadata management. Attendees will walk away with an action plan for their transformation and migration efforts.

HSCM04: SHAREPOINT'S SOCIAL COMPUTING SCORECARD

CHRISTIAN BUCKLEY

This session is a deep dive into the leading social networking contenders (Facebook, Ning, Wave, Jive, Box, etc), comparing and contrasting their capabilities against SharePoint 2010 capabilities, and why they are important to the enterprise. This session will catalog the rise of commercial social media tools, outline social media in the enterprise (business value, changes to social informatics in the workplace, data and intellectual property concerns), and present a scorecard of the primary features of the leading solutions against SharePoint 2010 features in the enterprise, with guidance on how to build comparable solutions in SharePoint, and with answers to concerns about security, IP rights, data management, network impact, and employee productivity. Attendees will walk away with a better understanding of what SharePoint 2010 is capable of, and some ideas for how they can augment their own designs and planning.

HSCM05: TRUST ME I AM A DEVELOPER: THINGS AN ADMIN SHOULD KNOW ABOUT DEVELOPING ON SHAREPOINT

DARRIN BISHOP

Let me tell you how it is. Well maybe how it should be. There are a lot of us developers in the wild now, and many of us are calling ourselves SharePoint developers. Can you tell the difference? Even though you might be an administrator, you should know enough about SharePoint development to call my bluff, because as a developer, well, sometimes I might try to sneak a thing or two past you. In this session we will discuss what you should be expecting from your SharePoint developers, things we tend to cheat on and how to keep us honest.

HSCM06: SHAREPOINT AS A PLATFORM FOR BUSINESS APPLICATIONS

OWEN ALLEN

SharePoint has grown into an extremely capable platform for the rapid construction and assembly of business applications. Learn about the components of the SharePoint platform that can be leveraged as elements of your business process management empire. See what a composite application is and how the combination of SharePoint Out-of-the-Box platform services and select third-party technologies can open a new frontier for business applications.

HSCM07: HORIZONTAL AND VERTICAL BUSINESS SOLUTIONS FOR SHAREPOINT 2010

OWEN ALLEN

A tour around the major types of technology solutions (gap fillers), horizontal business solutions, and vertical business solutions that are written for SharePoint 2007 and SharePoint 2010. What strategy should an enterprise develop to think about how to evaluate which applications and solutions would be appropriate to help meet the requirements of their business? We will review how to ensure that governance is maintained when multiple solutions are integrated within a SharePoint farm.

HSCM08: SHAREPOINT SOLUTIONS FOR INFORMATION TECHNOLOGY PROFESSIONALS

PAUL SWIDER

Many IT departments deploy SharePoint for the organization and overlook the business value of using collaboration internally. In this session, you will see examples of no code solutions created in SharePoint for IT departments.

EXCHANGE PRE-CONFERENCE WORKSHOPS

SUNDAY, MARCH 27, 2011 9AM - 4PM

EPR01: FILLING IN THE GAPS: EXCHANGE SERVER 2010 SP1 IN-DEPTH

(HANDS-ON WORKSHOP)

PETER O'DOWD & TOM PHILLIPS

Take this one day hands-on workshop to elevate your experience with Exchange Server 2010 SP1. In this workshop you'll be instructed by Wadeware Exchange gurus Peter O'Dowd (MVP) and Tom Phillips on the specifics of several key features of Exchange Server 2010 SP1. In this information-packed day you'll use a Hyper-V laptop provided by Microsoft to walk through several hands-on labs developed by Wadeware.

- Module 1: Exchange Server 2010 SP1 Overview
- Module 2: Exchange Server SP1 2010 Client Access (LAB: Client Access lab, including Mail-tips, Outlook Web App and OWA Themes, Personal Archive, External Calendar Sharing)
- Module 3: Exchange Server 2010 SP1 Information Leakage Protection and Control (LAB: Information Leakage Protection and Control, Litigation Hold, EDiscovery Preview Feature)
- Module 4: Exchange Server 2010 SP1 Management Tools & Role Based Access Control (LAB: Exchange Server 2010 SP1 Management Tools & RBAC)
- Module 5: Exchange Server 2010 SP1 Transport and Routing (LAB: Exchange Server 2010 SP1 Transport and Routing)
- Module 6: Exchange Server 2010 SP1 High Availability (LAB: Exchange Server 2010 SP1 High Availability)

EPR02: GET TO KNOW YOUR NEW BEST FRIEND, MICROSOFT LYNC SERVER 2010

(HANDS-ON WORKSHOP)

PAUL CHARBENEAU & THOMAS FOREMAN

Come take a hands-on guided tour of Microsoft Lync Server 2010 and see for yourself how Lync Server works to change communication within your organization. Much, much more than Instant Messaging, Lync Server provides IM, web conferencing, and Voice over IP solutions that allow you to increase your company's overall efficiency. In this information-packed day, you'll use a Hyper-V laptop provided by Microsoft to walk through several hands-on labs developed by Wadeware with OCS experts Thomas Foreman and Paul Charbeneau.

- Module 1: Lync Server 2010 Overview.
- Module 2: Lync Server 2010 Architecture, Planning and Deployment (LAB: The new management tools of Microsoft Lync Server 2010)
- Module 3: Lync Server 2010 Presence (LAB: The Microsoft Lync 2010 Unified Client)
- Module 4: Lync Server 2010 Voice Features (LAB: Microsoft Lync Server 2010 Enterprise Voice configuration)
- Module 5: Exchange 2010 SP1 Unified Messaging and Lync Server 2010 Integration (LAB: Configuring Exchange 2010 SP1 Unified Messaging and Lync Server 2010 integration)
- Module 6: Lync Server 2010 New Features (LAB: The Call Park Services and the new features of Lync Server 2010)

Space is limited, so sign up now!

WINDOWS PRE-CONFERENCE WORKSHOPS

SUNDAY, MARCH 27, 2011 9AM - 12PM

WPR01: AUTOMATING ACTIVE DIRECTORY ADMINISTRATION

MARK MINASI

Still administering your Active Directory the repetitive, click-and drag way? Lighten your workload with Windows Server 2008 R2's new PowerShell cmdlets. With these new cmdlets, you can often convert a task that once required a few hundred clicks—or two days of VBScripting—into just a few commands. What's that you say? You don't know PowerShell? No need to worry, as this workshop tosses in enough PowerShell basics to enable anyone comfortable with Active Directory to get productive with the AD PoSH cmdlets in no time. What's that you say? PowerShell doesn't look that exciting and so you're going to skip it? Well, if you do that, you'll miss out on a couple of R2's coolest new AD features, the AD Recycle

Bin and managed service accounts, both of which are basically impossible to use without some PowerShell. Look, when it comes to PowerShell, resistance is futile, so why not let veteran AD expert and explainer extraordinaire Mark Minasi take you on an easy-to-follow trip through R2's new cmdlets? We guarantee that every attendee will scratch his or her head and say, "Hey, I could use that!" at least once!

SUNDAY, MARCH 27, 2011 1PM - 4PM

WPR02: GROUP POLICY FUNDAMENTALS, SECURITY, AND CONTROL
JEREMY MOSKOWITZ

Group Policy is the most efficient way to manage desktops in a Windows environment. If you are still running to machines to install and configure desktops, you are not taking full advantage of the power of Group Policy. In this practical workshop, Jeremy Moskowitz will help you gain control of your environment and get your life back. This is the perfect workshop to take before doing "deep dives" into the main sessions of the conference. You'll get a little bit of everything: deployment, configuration, control, and security! We'll warm up with some Group Policy basics. Jeremy will show you how to manage your environment with GPOs, understand the differences between Group Policy and Group Policy Preferences, and show you the ropes of ADM and ADMX files. You'll get some "solid base hits" to ensure you can go back to work with some good ideas you can immediately put to use. For instance, learn how to zap printers down to your computers, and remotely deploy software to your users' desktops, and learn how to use Group Policy to secure collections of machines and lock down hardware. We'll examine how Group Policy can do the heavy lifting to the jobs you want to do! This session has both XP and Windows 7 content.

SUNDAY, MARCH 27, 2011 9AM - 4PM

WPR03: WINDOWS 7 DEPLOYMENT MASTER CLASS
RHONDA LAYFIELD

Learning Windows Deployment Tools can be quite a daunting task—where do you start and which one do you use? Windows Automated Installation Kit for Windows 7 (WAIK), Windows Deployment Service (WDS), Microsoft Deployment Toolkit 2010 Update 1 (MDT) or System Center Configuration Manager (SCCM)? The last thing you want to do is waste time learning a tool that's not right for you or your environment. Let Setup and Deployment MVP and Desktop Deployment Product Specialist Rhonda Layfield help you figure out which tool is right for you. In this full day deployment workshop, you'll learn how create, deploy and manage your images using the Windows Automated Installation Kit for Windows 7 (ImageX, DISM, CopyPE, OSCDImg, USMT 4.0). Perform bare metal installations using WDS—learn to install, configure and troubleshoot WDS. Migrate your XP machines to Windows 7 using the MDT 2010 Update 1. Then there's the golden tool—SCCM—which allows you to perform zero touch installations. More importantly, learn the differences between these tools so you can make your deployment solution work for you.

SHAREPOINT PRE-CONFERENCE WORKSHOPS
SUNDAY, MARCH 27, 2011 9AM - 4PM

HPR01: SHAREPOINT 2010 PROFESSIONAL DEVELOPMENT
ROBERT L. BOGUE & ERIC SCHUPPS

Go to www.devconnections.com for complete abstract.

HPR02: DAN HOLME'S SHAREPOINT COLLABORATION MASTERCLASS
DAN HOLME

Go to www.devconnections.com for complete abstract.

EXCHANGE POST-CONFERENCE WORKSHOPS
THURSDAY, MARCH 31, 2011 9AM - 4PM

EPS01: COLLABORATION USING SHAREPOINT 2010, EXCHANGE SERVER 2010 SP1, AND LYNC SERVER 2010 (HANDS-ON WORKSHOP)
PETER O'DOWD & PAUL CHARBENEAU

With your head packed full of valuable information from a week of UC sessions, put it all together in this one-day workshop that shows how to integrate Exchange Server 2010, Lync Server 2010, and SharePoint Server 2010. This instructor led hands-on-lab experience will get you deep into Exchange and guide you through these features, showing you how they are configured and how they can be used to improve your organization's Unified Communications platform.

- Module 1: Overview of SharePoint 2010 Integration Features (LAB: Using My Site and Office Web App for SharePoint)
- Module 2: Integrating SharePoint with Exchange Server 2010 SP1 (LAB: Integrating SharePoint with Outlook and Exchange Server 2010 SP1)
- Module 3: Integrating SharePoint Workspaces with Outlook and Exchange Server 2010 SP1 (LAB: Integrating SharePoint Workspaces with Outlook and Exchange Server 2010 SP1)
- Module 4: Integrating SharePoint with Lync Server 2010 (LAB: Integrating SharePoint with Lync Server 2010 and Active Feed)
- Module 5: Integrating Exchange and Lync Server 2010 (LAB: Integrating Exchange OWA and Lync Server)

No need to bring your laptop, hardware will be provided by Microsoft for this event. Space is limited, so sign up now!

WINDOWS POST-CONFERENCE WORKSHOP
THURSDAY, MARCH 31, 2011 9AM - 12PM

WPS01: MIGRATING AND RESTRUCTURING YOUR AD
J. PETER BRUZZESE

Support for Windows 2000 ended mid-2010 and the result is an overwhelming number of IT shops looking to migrate their existing domain infrastructure over to Server 2008/2008 R2. In addition, many are in need of a major restructuring of their forests because they were initially created with a domain overkill approach due to the constraints of legacy AD versions. In this workshop we will begin by walking through several tools to aid you with the migration/restructure and then focus on the one with the best price tag, the Active Directory Migration Tool (ADMT), which is free incidentally. Using a huge case study which included a migration of 65,000 users and computers from 65 locations and 65 different forests into a single forest with 20 domains, we will discuss all the planning necessities, caveats to avoid, and all of the key focus points to ensure your migration goes smoothly.

SHAREPOINT POST-CONFERENCE WORKSHOPS
THURSDAY, MARCH 31, 2011 9AM - 4PM

HPS01: BUSINESS CONNECTIVITY DEEP DIVE
SCOT HILLIER & TODD BAGINSKI

Go to www.devconnections.com for complete abstract.

HPS02: ORGANIZING INFORMATION IN SHAREPOINT SERVER 2010
BILL ENGLISH

Go to www.devconnections.com for complete abstract.

NOTE: LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS. THE COST OF A WORKSHOP IS IN ADDITION TO THE REGULAR CONFERENCE FEE

Check Web site for Microsoft and additional speakers.

A UNIQUE OPPORTUNITY TO GET YOUR TECHNOLOGY AND TRAINING FROM MICROSOFT AND INDUSTRY EXPERTS!

SPEAKERS

OWEN ALLEN
SHAREPOINT DIRECTIONS LLC

TODD BAGINSKI
FRESH TRACKS CONSULTING, LLC

ROBERT BEAUCHEMIN
SQLSKILLS.COM

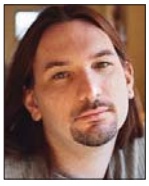
DARRIN BISHOP
KNOWLEDGELAKE, INC.

ROBERT L. BOGUE
THOR PROJECTS

J. PETER BRUZZESE
CLIPTRAINING

CHRISTIAN BUCKLEY
AXCELER

PAUL CHARBINEAU
WADEWARE



DENNY CHERRY

MIKE CROWLEY
PLANET TECHNOLOGIES, INC.

BEN CURRY
SUMMIT 7 SYSTEMS

MIKE DANSEGLIO
CONCENTRATED TECHNOLOGY

SEAN DEUBY
WINDOWS IT PRO

CATHY DEW
SUMMIT 7 SYSTEMS

BILL ENGLISH
MINDSHARP

THOMAS FOREMAN
WADEWARE

DEVIN L. GANGER
CONSULTANT/ AUTHOR

SCOT HILLIER
SCOT HILLIER TECHNICAL SOLUTIONS, LLC

JOHN HOLLIDAY
JOHN HOLLIDAY & ASSOCIATES, INC.

DAN HOLME
INTELLIEM, INC.

LAURA HUNTER
MICROSOFT

VICTOR ISAKOV
ITIL V3 FOUNDATIONS

DON JONES
CONCENTRATED TECHNOLOGY

KEVIN LAAHS
HP

RHONDA LAYFIELD
DEPLOYMENTDR.COM

ANDY LEONARD
ANDY LEONARD TRAINING

PAUL LITWIN
DEEP TRAINING

JIM MCBEE
ITHICOS SOLUTIONS

KIERAN MCCORRY
HP

MATTHEW MCDERMOTT
ABLEBLUE

MARK MINASI
MINASI RESEARCH AND DEVELOPMENT

JEREMY MOSKOWITS
MOSKOWITZ, INC.

MICHAEL NOEL
CONVERGENT COMPUTING

PETER O'DOWD
DATACOM/ WADEWARE

BRENT OZAR
SQLSKILLS.COM

JOEL OLESON
QUEST SOFTWARE

TED PATTISON
CRITICAL PATH TRAINING

MACIE J. PILECKI
PROJECT BOTTICELLI LTD

TOM PHILLIPS
WADEWARE

MAURICE PRATHER
INDEPENDENT CONSULTANT

PAUL S. RANDAL
SQLSKILLS.COM

ASIF REHMANI
SHAREPOINT-ELEARNING.COM

ERIC SCHUPPS
BINARYWAVE

GREG SHIELDS
CONCENTRATED TECHNOLOGY

MICHAEL B. SMITH
THE ESSENTIAL EXCHANGE

ALAN SUGANO
ADS CONSULTING GROUP

PAUL SWIDER
OCS, LLC

KIMBERLY L. TRIPP
SQLSKILLS.COM

JW Marriott Orlando Grande Lakes
4040 Central Florida Parkway
Orlando, FL 32837

TAX DEDUCTION

Your attendance to the conference may be tax deductible.
Visit www.irs.ustreas.gov. Look for topic 513 - Educational Expenses. You may be able to deduct the conference fee if you undertake to (1) maintain or improve skills required in your present job; (2) fulfill an employment condition mandated by your employer to keep your salary, status, or job.

GROUP DISCOUNT

Register individuals from one company at the same time and receive a group discount.

1-3 registrants	**$1,595 per person**
Additional registrants after the 3rd (4th, 5th, 6th...)	**$1,395 per person** ($200 off each)

Call 800-438-6720 to take advantage of group discount pricing.

Join us!

JW Marriott Orlando Grande Lakes

The JW Marriott Orlando, Grande Lakes provides all of the comfort and variety you could imagine. From the moment you are welcomed by our signature Spanish fountain, you'll know that you have found one of the most prestigious hotels in Orlando, Florida. Conveniently located near Universal Orlando®, SeaWorld®, and Walt Disney World® and other exciting local attractions, our hotel transports guests to a place of unsurpassed serenity and beauty, including:

- Access to The Ritz-Carlton Golf Club and Spa
- Lazy River outdoor heated pool

Space is limited so reserve your room early by calling the conference hotline. Call the conference hotline at 800-438-6720 or 203-400-6121 to reserve your rooms today!

The special conference rate will be honored starting two days before the start of conference through two days after the end of the conference, **based upon availability**. Space is limited so reserve your room early by calling the conference hotline at 800-438-6720 or 203-400-6121. All reservations must be guaranteed with a major credit card to confirm room.
Parking at the hotel: Daily Self-parking is $17.04 and daily valet parking is $23.43 (subject to change)

AIRLINE

Please call Pericas Travel at 203-562-6668 for airline reservations.

AIRLINE SHUTTLE

Mears Transportation is the designated ground carrier at Orlando International Airport. The shuttle maybe picked up at Level 1 of the airport. Visit www.mearstransportation.com for reservations. Rates: $19.00 one-way and $30.00 roundtrip (subject to change)

CAR RENTAL

Hertz is offering auto rental discounts to attendees. See Web site for details.

ATTIRE

The recommended dress for the conference is casual and comfortable. Please bring along a sweater or jacket, as the ballrooms can get cool with the hotel's air conditioning.

Sponsorship/exhibit information For sponsorship information, contact Rod Dunlap 480-917-3527 or rod@devconnections.com
See Web site for more details: www.WinConnections.com

CONFERENCE REGISTRATION • MARCH 27-30, 2011

FULL CONFERENCE REGISTRATION INCLUDES KEYNOTE ON MARCH 27, 2011
THROUGH CLOSING SESSION MARCH 30TH, 4:30PM

NAME _____ PRIORITY CODE _____

COMPANY _____ TITLE _____

STREET ADDRESS (REQUIRED TO SHIP MATERIALS) _____

CITY, STATE, POSTAL CODE _____ COUNTRY _____

TELEPHONE _____ FAX _____ E-MAIL ADDRESS (IMPORTANT) _____

ONLINE: www.WinConnections.com
E-MAIL: info@WinConnections.com
PHONE: (800) 438-6720
(203) 400-6121
FAX: (913) 514-9362
MAIL:
Penton Media
731 Main Street Ste C3
Monroe CT 06468

☐ **Microsoft Exchange Connections**
☐ **Windows Connections**
☐ **SharePoint Connections**

On or Before February 1st, 2011 ..... $1495 _____
After February 1st, 2011 ..... $1595 _____

FOR WHICH CONFERENCE ARE YOU REGISTERING? _____

PRE-CONFERENCE WORKSHOPS SUNDAY, MARCH 27, 2011 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

☐ EPR01: FILLING IN THE GAPS: EXCHANGE SERVER 2010 SP1 IN-DEPTH
(HANDS-ON WORKSHOP) O'DOWD & PHILLIPS ..... 9AM - 4PM ..... $425 _____

☐ EPR02: GET TO KNOW YOUR NEW BEST FRIEND, MICROSOFT LYNC SERVER 2010
(HANDS-ON WORKSHOP) CHARBENEAU & FOREMAN ..... 9AM - 4PM ..... $425 _____

☐ WPR01: AUTOMATING ACTIVE DIRECTORY ADMINISTRATION MINASI ..... 9AM - 12PM ..... $199 _____

☐ WPR02: GROUP POLICY FUNDAMENTALS, SECURITY, AND CONTROL MOSKOWITZ ..... 1PM - 4PM ..... $199 _____

☐ WPR03: WINDOWS 7 DEPLOYMENT MASTER CLASS LAYFIELD ..... 9AM - 4PM ..... $399 _____

☐ HPR01: SHAREPOINT 2010 PROFESSIONAL DEVELOPMENT BOGUE & SCHUPPS ..... 9AM - 4PM ..... $399 _____

☐ HPR02: DAN HOLME'S SHAREPOINT COLLABORATION MASTERCLASS HOLME ..... 9AM - 4PM ..... $399 _____

POST-CONFERENCE WORKSHOPS THURSDAY, MARCH 31, 2011 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

☐ EPS01: COLLABORATION USING SHAREPOINT 2010, EXCHANGE SERVER 2010 SP1, AND LYNC SERVER 2010
(HANDS-ON WORKSHOP) O'DOWD & CHARBENEAU ..... 9AM - 4PM ..... $425 _____

☐ WPS01: MIGRATING AND RESTRUCTURING YOUR AD BRUZZESE ..... 9AM - 12PM ..... $199 _____

☐ HPS01: BUSINESS CONNECTIVITY DEEP DIVE HILLIER & BAGINSKI ..... 9AM - 4PM ..... $399 _____

☐ HPS02: ORGANIZING INFORMATION IN SHAREPOINT SERVER 2010 ENGLISH ..... 9AM - 4PM ..... $399 _____

CONFERENCE MATERIALS

FULL CONFERENCE REGISTRATION INCLUDES MATERIALS FOR THE CONFERENCE FOR WHICH YOU REGISTER; YOU MAY PURCHASE MATERIALS FOR THE OTHER CONCURRENTLY RUN EVENTS.

☐ Microsoft Exchange Connections Conference CD ..... $75 _____
☐ Windows Connections Conference CD ..... $75 _____
☐ SharePoint Connections Conference CD ..... $75 _____

TOTAL

☐ CHECKS (payable to Penton Media)) All payments must be in US Currency. Checks must be drawn on a US bank.

☐ CREDIT CARD ☐ VISA ☐ MASTERCARD ☐ AMEX

CREDIT CARD NO. | | | | | | | | | | | | | | | | |

EXPIRATION DATE | | | | | | |

_____
Cardholder's Signature Cardholder's Name (print)

Penton Media
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

Mailroom: If addressee is no longer here,
please route to MIS Manager or Training Director

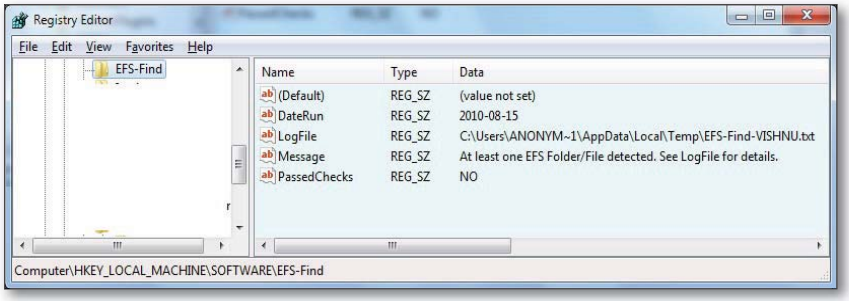


Figure 2: Writing information to the registry

folder on the Windows Server 2003 CD-ROM. You can use this tool to find all encrypted folders and files on your computer, but it typically produces a blizzard of information that's difficult to plow through. For example, try issuing the following command at the root of your C drive:

```
Efsinfo /S:C:
```

All the filenames and folder names go blasting across your screen, so it's like looking for a needle in a haystack. You can display only those lines that contain the string ": Encrypted" by running the command

```
Efsinfo /S:C: | Find ": Encrypted"
```

Now you at least get some filtered results such as

```
EFS-Test.txt: Encrypted
EFS-Test: Encrypted
```

But, sadly, the results don't include the paths to the encrypted folders and files. (Maybe a newer version of the EFSinfo tool does, but I couldn't get the version I was using to give up this information.)

Using Cipher

A more suitable way to find encrypted folders and files is to use Cipher. This powerful command-line utility has many encryption and decryption options for managing the encryption environment. You can also use it to determine whether any encrypted files exist on your computer. For example, the command

```
Cipher /U /N
```

checks for encrypted files on your computer and displays any it finds. As these results show,

```
Encrypted File(s) on your system:
C:\Program Files\EFS-Test.txt
```

the file's full path is included. However, in all the tests I conducted in Windows 7, the results didn't include the empty encrypted folder.

Using EFS-Find.vbs

When you can't get off-the-shelf tools to do exactly what you want, it's time to see what good old VBScript can do. That's how EFS-Find.vbs came into being. EFS-Find.vbs locates all encrypted folders and files on your hard disk and automatically saves their complete paths to a log file.

You can download EFS-Find.vbs by going to www.windowsitpro.com, entering 129393 in the InstantDoc ID box, clicking Go, then clicking the *Download the Code Here* button. Save the script to a location on your computer (in this example, C:\Test\EFS-Find.vbs), then open a command prompt window as an administer and run the command

```
Cscript //NOLOGO
  C:\Test\EFS-Find.vbs
```

(Although this command wraps here, you'd enter it all on one line.) The script will search all the local hard drives on your computer and report on any EFS folders and files it finds. Unlike the Cipher /U /N command, EFS-Find.vbs reports on any empty encrypted folders.

Besides displaying a summary report on screen, the script displays the log file's name, which is in the format EFS-Find-%COMPUTERNAME%.txt. This naming convention makes it easy to distinguish between different computers if you need to push the files to a central location without them being overwritten. The log file is saved to the directory specified in the %TEMP% environment variable, which is usually the current user's temporary folder.

Here's how EFS-Find.vbs works. It begins by making sure that you're a local administrator so that it can run properly. Then, for each fixed drive, it performs two checks. First, it checks each folder to see if it's encrypted. It does this by taking advantage of Windows Management Instrumentation's (WMI's) Win32_Directory class. Second, it checks each file to see if it's encrypted using WMI's CIM_DataFile class. The script writes the results to the log file, which it opens before quitting. If you aren't running the script interactively, you can disable this feature. Find the code

```
objShell.Run """" _
  & strLogFileName & """"
```

and comment it out.

The script also writes information to the registry at HKLM\SOFTWARE\EFS-Find, as Figure 2 shows. That way, there's always a fixed location to query the computer about the script's status. In addition, you can be certain of the computer's encryption status on that particular date.

EFS-Find.vbs returns an error level that you can check if desired. Simply execute the following command in the same command prompt window you used to run the script

```
ECHO %ERRORLEVEL%
```

An error level of 10 indicates the script exited because it wasn't run under elevated permissions (i.e., as an administrator). An error level of 999 indicates at least one EFS folder or file was detected. If the script returns an error level of 0, no EFS folders or files were detected.

If the script detects EFS folders and files, you can navigate to them using the paths provided in the log file and decrypt or remove them. Afterward, you can rerun EFS-Find.vbs and the error level check to confirm that no EFS folders or files exist.

Finding EFS Folders and Files the Easy Way

With EFS-Find.vbs, you can accurately determine whether there are any EFS folders and files on a computer. Plus, it checks all the fixed drives on a computer in the same run, so it's quick and easy. Whether you run it interactively or build it into a wrapper, you'll know for certain that no EFS folders or files exist.

—Harry Verge, senior technology specialist

InstantDoc ID 129393

- Outlook
- Task Manager
- Active Directory
- Virtual Hard Disks

ANSWERS TO YOUR QUESTIONS

Q: I have a process that I can't kill. What can I do?

A: If you've tried to stop a process using Task Manager, taskkill /f from the command line, and even the Sysinternals tool PsKill (available from Microsoft at bit.ly/CB2X2), but the process is still running, it's likely become stuck in kernel mode and can't be stopped. This is a time when trying a reboot is realistically your only choice.

—John Savill

InstantDoc ID 129435

Q: How can I stop people from using Reply All on messages I send them?

A: Accidentally selecting Reply All on a multi-recipient message you've received can be a career-limiting move, or at least annoying when the message was addressed to hundreds—if not thousands, or tens of thousands—of recipients buried in distribution groups. You can already disable Reply All for users; however, a new add-in from Microsoft Research gives the sender control of whether recipients of the message can use Reply All.

Microsoft Research developed a form (made public recently) that lets the sender of a message block the recipients from using Reply All or Forward. You can download the small (~300KB) file from Microsoft's website at bit.ly/aYJUi7.

The NoReplyAll add-in requires a very simple installation accomplished by launching setup.exe. It has three prerequisites in addition to either Outlook 2010 or Outlook 2007: Windows Installer 4.5, Microsoft .NET Framework 4 Client, and Microsoft Visual Studio 2010 Tools for Office Runtime. If any of these applications aren't present, the NoReplyAll setup downloads and initiates the installation—after you accept the EULA—for each missing application.

After installing the add-in, you can launch Outlook to show that it has been applied. Select the Office Backstage view by clicking the File tab with Outlook 2010 opened. Next, select Options, then Add-Ins in the left column. NoReplyAllAddin should be visible in the list if it installed successfully.

Now when you create an email message, you'll see a new section in the Outlook Ribbon, which lets you prevent recipients from using Reply All and Forward, as Figure 1 shows. Selecting these options disables the functionality for the recipient—the buttons to Reply All and Forward are grayed out. Interestingly, if the message is previewed in the Reading Pane rather than opened in its own window, the Reply All and Forward buttons remain enabled; however, if the user selects them, an error message states that such an action isn't available.

This behavior is the result of a macro accompanying the message; it isn't specific to the user, as a Group Policy setting is. Every recipient of this message has this functionality disabled for this message. The VBA code that disables the options is

```
ActiveInspector.CurrentItem
  .Actions("Reply to All").Enabled =
  False
ActiveInspector.CurrentItem
  .Actions("Forward").Enabled = False
```

With the NoReplyAll add-in, senders can easily control the ability of recipients to use Reply All on a message-by-message basis. This feature works as long as the email client used is Outlook 2010 or Outlook 2007, with or without Exchange Server.

—William Lefkovics

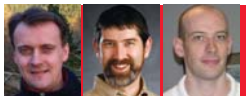
InstantDoc ID 129469

Q: If I want to boot from a Virtual Hard Disk (VHD), does my processor have to support virtualization?

A: Boot from VHD (or VHD with Native Boot) is a new feature of Windows 7 (Enterprise and Ultimate editions) and Windows Server 2008 R2 that allows a physical machine to boot from an OS stored inside a VHD. Although it might seem like virtualization is used, you're not actually performing machine virtualization (where the OS is abstracted from the physical hardware). You typically only need processor virtualization support (Intel VT or AMD-V) for machine virtualization. All you're doing with boot from VHD is using file system virtualization capabilities, which means your processor doesn't have to support virtualization to boot from a VHD.

—John Savill

InstantDoc ID 129361



Jan De Clercq | jan.declercq@hp.com
William Lefkovics | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com

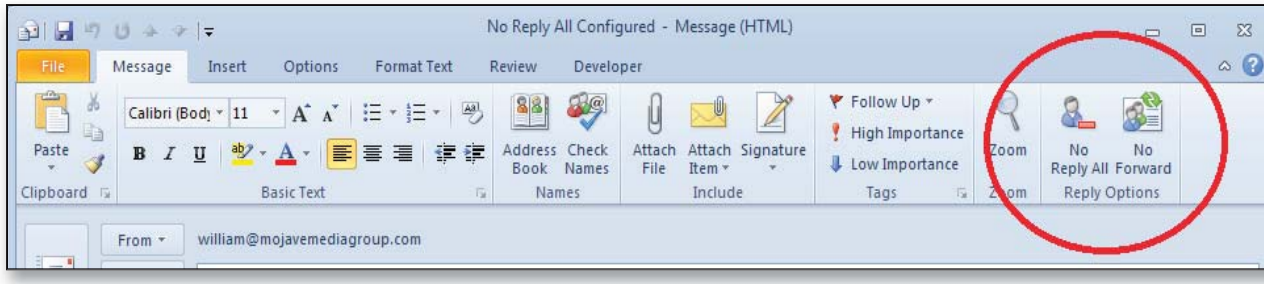


Figure 1: No Reply All and No Forward options on a new mail window

Q: How can I make sure that only the authorized administrator group for a given organization can view its organizational unit (OU)?

A: AD has four Read permissions: List Contents, Read All Properties, Read Permissions and List Object. The first three are enabled and visible by default. List Object isn't visible or enabled by default.

Say you're running a shared Active Directory (AD) setup in a hosting solution where different organizations share the same AD domain. In your environment, it's important to ensure that only an organization's authorized administrators can access the AD information and configuration settings of their organization.

For that purpose, you create different AD administrator groups (called Admins_CompanyA, Admins_CompanyB, and so on). The organization's OUs are created underneath a parent OU called UserAccounts. How can you make sure that only the authorized administrator group for a given organization can view the content of its organization's OU (called, for example, CompanyA, CompanyB, CompanyC)?

The List Contents permission normally lists all immediate child objects. With the List Object permission enabled, AD can hide objects that are returned by the List Contents function. The List Object permission isn't active or visible in AD's ACL editor until the List Object mode in the forest has been enabled. Once the feature is enabled, a new permission—List Object—will appear in an AD object's ACL Editor.

The concept of the List Object permission is quite simple. Without it, when a user queries a container's contents in AD, AD doesn't evaluate the permissions of any objects underneath the container object (such as an OU). If the user hasn't been granted the List Contents permission on the OU, no child objects are returned to the user from AD. And once the user has been granted the List Contents permission on the OU, AD will return all child objects of that OU to the user—regardless of whether the user has read permission or is even denied access to the child object.

With List Object mode enabled, administrators can remove or deny the List Contents permission on a parent container and AD will still process the permissions on the child objects of the container to check if the user has been granted the List Object permission on any child object. If so, AD will add the object to the result set. If not, the object will be omitted.

List Object permissions are ideally suited for situations where users aren't supposed to see certain objects in AD at all. They're typically used on OUs to fully remove their visibility for all OU administrators, except for the ones responsible to manage that particular OU. The List Object permission is mostly helpful in outsourcing environments.

Within an organization, the List Object permission is often used to hide security-sensitive objects, such as admin accounts, from unauthorized users, mainly to limit the potential for DOS attacks against these accounts.

To enable AD's List Object mode, you must edit a property of the Directory Services object in the configuration container of AD. This will replicate to all other domain controllers (DCs) in the forest and notify them of the change. It's not possible to activate the mode on a per-domain basis.

You can activate List Object mode by setting the third character of the DSHeuristics property on the Directory Service object to 1. If the DSHeuristics property hasn't been set with other values, set it to 001. (If the first two characters are already set to non-zero values, leave them as they are.) The Directory Service object is located at cn=Directory Service,cn=Windows NT,cn=Services,cn=Configuration, dc=ForestRootDomain. To set AD to List Object mode, you can use the ADSIEdit MMC tool.

In the above example, you should follow these steps to enable only authorized users (members of the groups Admins_CompanyX) to view their respective OUs (CompanyA, CompanyB, CompanyC) underneath a parent OU called UserAccounts:

1. Remove the default List Contents permission for Authenticated Users from the UserAccounts OU (so that permissions of child objects are evaluated).
2. Remove the default List Object permission for Authenticated Users from all Company OUs to hide visibility of Company OUs themselves. In addition, AD will remove List Contents from the OU to hide the objects within them (so that they're also not returned via an LDAP query).
3. Grant the List Object and List Contents permission for each Admins_CompanyX group on the respective Company OU.

In summary, there are two important things to remember when working with the List Object mode in AD. First, List Object mode can be enabled only for a whole AD forest—it's not possible to enable it per domain. Second, to use the List Object permission on child objects, the List Contents permission for Authenticated Users should be removed from the respective parent container. If a user is granted the List Contents permission on a container object, the objects inside will be visible no matter what the underlying List Object permissions of the child objects are.

—Jan De Clercq

InstantDoc ID 129486

The Conversation Begins **Here**

APRIL 17-20, 2011
BELLAGIO, LAS VEGAS

mobile connections | cloud connections | virtualization connections

Questions Answered • Strategies Defined • Relationships Built

NOWHERE ELSE WILL YOU FIND THIS MANY
INDUSTRY EXPERTS

Jay Freeman
CYDIA

Tyler Lassard
RIM

John Stetic
NOVELL

Joe Belfiore
MICROSOFT

Jim Reavis
CLOUD SECURITY ALLIANCE

Emerging trends in cloud computing

How to build, market, and deliver apps seamlessly

How current and future virtualization products will help shape the future of cloud computing

NETWORK WITH YOUR PEERS!

Network with your peers, carriers and a wide range of mobile infrastructure, product and service vendors! Get bet-the-business market knowledge for business leaders, developers and IT managers exploring or implementing cross-platform mobile development, cloud computing and virtualization.

50+ SPEAKERS!
8 KEYNOTE PRESENTATIONS
60+ BREAKOUT SESSIONS
12 BOOT CAMPS

Brought to you by: connected planet | DEVCONNECTIONS | SQL SERVER | Windows IT Pro

3 CONFERENCES - 1-STOP EXPO - GREAT NETWORKING

REGISTER FOR 1 EVENT, GAIN ACCESS TO ALL 3!

Ric Telford
IBM CLOUD SERVICES

Robert Scoble
RACKSPACE

Jinesh Varia
AMAZON WEB SERVICES

Nils Puhlmann
ZYNGA

Ilja Laurs
GETJAR

Getting optimal business efficiency using Microsoft and VMware virtualization solutions

Description of mobile panel: Which platform do you bet on?

ROI of implementing cloud and virtualization platforms and solutions

Aaron Hillegass
BIG NERD RANCH

Michele Leroux Bustamante
IDESIGN INC.

Paul Thurrott
WINDOWS IT PRO

Steve Riley
RIVERBED TECHNOLOGY

Pamela Dingle
PING IDENTITY

Ryan O'Hara
MICROSOFT

REGISTER TODAY!

TheConversationBeginsHere.com or call 800.505.1201

COVER STORY

Troubleshooting DNS in the New Decade

Simplify name resolution on your network

by Mark Minasi

Got an Active Directory (AD) problem? Chances are, it's really a DNS problem. Can't get to your email, Twitter, or Facebook account? Chances are, it's really a DNS problem. Smoking out DNS-related problems is Step Two in troubleshooting almost any network problem—but knowing how to troubleshoot DNS is something of a moving target, because it just keeps changing. We've covered the basics of DNS troubleshooting in the past. (See the Learning Path.) In this article, we move beyond the basics to take a new look at an old idea. We explore how to simplify name resolution with a couple of DNS troubleshooting tools that far surpass Nslookup, and we examine in-depth the unjustly accused cause of a DNS trouble scenario that's new in Windows Server 2008 R2: Extension Mechanisms for DNS (EDNS).

Turn Off WINS

When people say, "Check DNS," it's sort of shorthand for "Check the entire name resolution infrastructure," which includes local NetBIOS broadcasts, WINS, and a newly styled Network Neighborhood replacement called Network Discovery that arrived with Windows Vista—not to mention the HOSTS and LMHOSTS files. No wonder name resolution troubleshooting is so complicated! It's as if some of your electricity came from the phone company and ran at 80 volts, some came from the cable company and provided direct current, and the rest came from the traditional power company, but you never knew exactly which kind of power went to your blender, your computer, or Grandma's iron lung—which would make troubleshooting nonworking appliances very difficult and time consuming. Simplify the name resolution, and the troubleshooting gets easier.

Before you turn off WINS, you should of course test your network configuration without it (including the NetBIOS over TCP/IP setting in your TCP/IP properties). I think you'll be surprised by how few things—or nothing at all—still need WINS, although it clearly depends on how modern your client and server OSs are. Disabling WINS is a terrible idea in Windows 2000 Server, workable but occasionally annoying in Windows Server 2003 and Windows XP, and fairly trouble-free in Vista and later OSs. Understand, however, that just because your OS is fine in a NetBIOS-free environment, your apps might not be—I've heard that some anti-malware apps need NetBIOS, although I haven't run into this situation. If you do need WINS for an occasional app or two, look into using Server 2008's GlobalNames zone; it can help DNS do part of WINS's job. (For more information about Server 2008's GlobalNames zone, see "What is GlobalNames in Windows Server 2008?" InstantDoc ID 96872.)

Use Network Monitor

Everyone knows about Network Monitor, but most folks are still scared to try it—and they shouldn't be. Network Monitor captures and displays every network packet that enters or leaves your system, laying bare for your inspection every single bit that zips through your NIC. Netmon initially seems like a tool for black belts, but in some ways it's even better suited for the Jack-of-all-trades DNS troubleshooter

Learning Path

***WINDOWS IT PRO* RESOURCES:**

"Identify and Troubleshoot DNS Problems," InstantDoc ID 125990

"DNS Enhancements in Windows Server 2008 R2," InstantDoc ID 125360

"Deconstructing DNS," InstantDoc ID 48527

"How DNS Works," InstantDoc ID 8666

"A DNS Primer," InstantDoc ID 7733

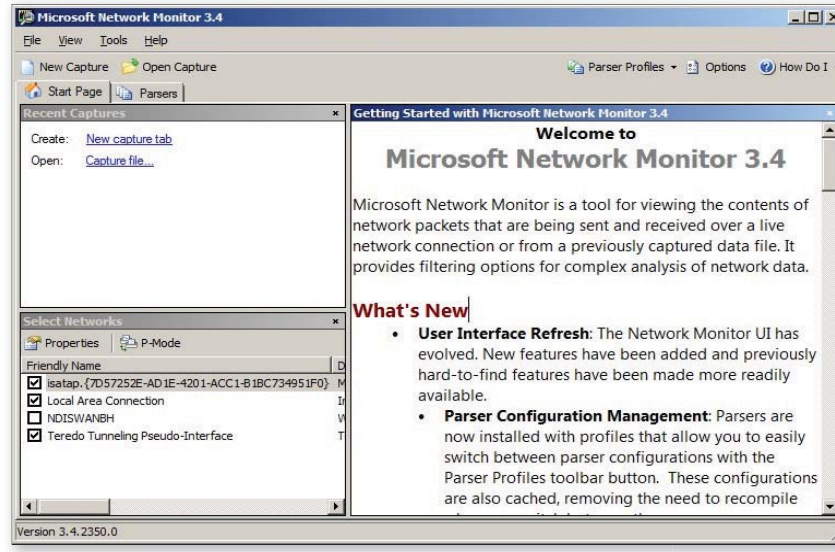


Figure 1: Network Monitor's welcome screen

because it lets administrators employ an old repair adage: It's hard to recognize "sick" if you don't know what "healthy" looks like. So if you run Netmon on your system when it's working, keep that capture handy and then run another capture when things aren't working. Compare the two captures and play a bit of "What's different?" and you'll soon start gleaning clues.

I know that simply mentioning Netmon causes some folks to run in fear, but don't—here's a quick primer on Netmon and DNS. In this example, I set up a Server 2008 R2 DNS server, which I configured to look to itself to resolve DNS addresses. I told the server to ping www.bigfirm.com and capture the resulting network traffic with Netmon. The result will be a complete mess of largely irrelevant network chatter—a ton of ore from which we want to pluck just a few golden nuggets.

The first step is to install Network Monitor. (The tool is available for free download from www.microsoft.com/downloads/en/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f.) When you start Netmon, be sure to right-click its icon and select *Run as administrator.* The first time you start Netmon, the program asks whether you want to use Microsoft Update. After you dismiss this dialog box, you'll see a welcome screen such as the one in Figure 1. The lower left window controls which traffic you want captured. We don't care about the isatap and Teredo traffic, so clear those check boxes. Leave the Local Area Connection check box selected. Ignore the P-Mode option; enabling it would only add to the clutter. Click *New capture tab* in the upper left window.

The Capture screen that opens, which Figure 2 shows, is one of the reasons administrators shy away from Netmon. To simplify this screen, close the Network Conversation pane on the far left side and the Hex Details pane in the lower right corner, leaving just Display Filter, Frame Summary, and Frame Details.

To put Netmon to work, open a command prompt and click the green triangle next to Start in the Netmon window. Give Netmon a second to get rolling, then return to the command prompt and run

```
ping -n 1 www.bigfirm.com
```

After the Ping command runs, return to Netmon and click the blue square next to Stop. Congratulations—you've made your first capture! Look at the status information at the very bottom of the Netmon window frame to see how many network packets you captured. Depending on how quickly you worked and how quiet your network is, you might have anywhere from about a dozen frames to a hundred or so. No matter how many you have, it'll look like a mess. To separate the wheat from the chaff, you need to create a display filter.

To view only the DNS-specific traffic, enter *DNS* in the Display Filter text field and click Apply. You'll see a screen such as the one in Figure 3. This example screenshot shows just the six packets I'm interested in. (I removed the Process, Time Offset, and TimeDateLocalAdjusted columns because they weren't relevant to this capture.)

These six packets show how a DNS server finds basically any host in any .com

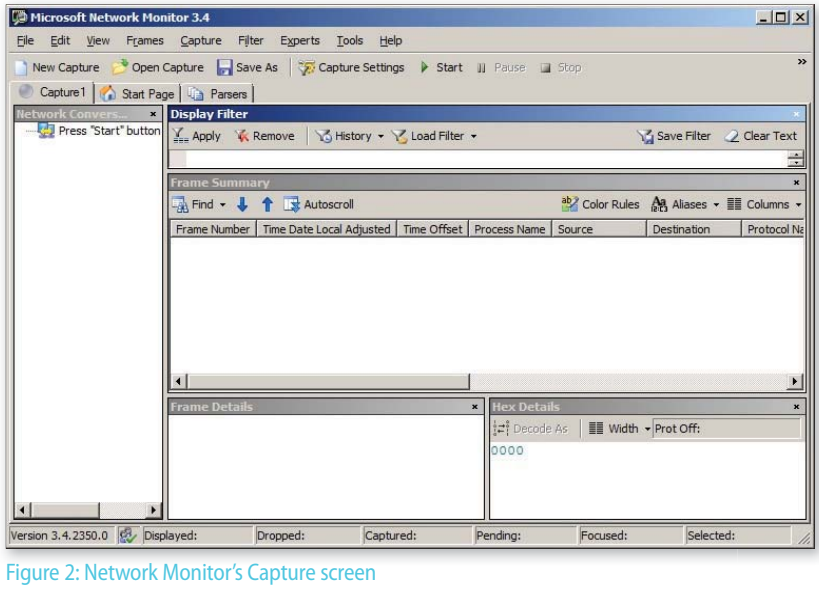


Figure 2: Network Monitor's Capture screen

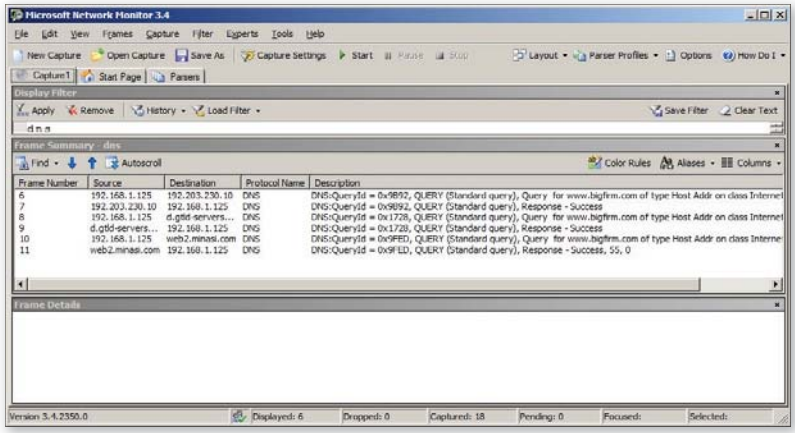


Figure 3: Viewing DNS-specific traffic

domain. First, your local DNS server queries a root server for the host address of www.bigfirm.com (packet 6, notice "Query for www.bigfirm.com…"). The root server responds, "I have no idea, but if you ask one of the .com DNS servers, it can help you" (packet 7, notice "Response—Success"). Then your DNS server asks a .com DNS server for www.bigfirm.com's host address (packet 8) and is told that no, the .com DNS server can't help, but that your DNS server might try asking bigfirm.com's DNS server (packet 9). Your DNS server then asks bigfirm.com's DNS server for www.bigfirm.com's host address (packet 10) and finally gets its desired response (packet 11). Note that Netmon makes keeping track of who's doing the talking easier with its Source and Destination columns: My local DNS server is 19.168.1.125, the root server is 192.203.230.10, the .com DNS server is d.gtld-servers, and bigfirm.com's DNS server is web2.minasi.com. This is, of course, a very high-level overview.

To view a packet's hierarchy, click the first of the filtered frames and look in the Frame Details pane. Figure 4 shows the packet hierarchy, which Netmon calls a frame. This frame contains the Ethernet packet, which in turn contains the IPv4 packet. Within IPv4 is the UDP packet (it could be TCP, but most DNS traffic runs over UDP), and inside that is the actual DNS query. Each level's summary includes relevant addresses or ports and lengths for a nice overview. To dig deeper into the DNS query, click the plus sign to expand the DNS frame, as Figure 5 shows. Netmon's level of detail in this frame is fairly self-explanatory. You can see that it's a query (rather than a response), the question (host record for www.bigfirm.com), and an additional record that I'll cover later in the article.

In the next frame's DNS details you'll see that the root server responds by telling your DNS server, "Go talk to a .com DNS server," by simply returning the list of 13 .com DNS servers. Your DNS server makes the same query to the .com DNS servers, recursing through the DNS hierarchy until your DNS server finally gets its answer.

So how does this information help you troubleshoot DNS problems? Well, just recently, one of my DNS servers simply stopped responding to DNS queries. To make matters worse, a look at the detailed logging that Windows DNS servers can offer showed that the DNS server hadn't received any queries. Could the firewall have somehow started blocking DNS traffic? The fastest way to find out was to run Netmon, which showed me that yes, indeed, the NIC was receiving the DNS queries from other systems—I could see the frames, and I could see that my DNS server had responded to none of them. I was confident that it wasn't a DNS problem, but rather something in the routing and IP itself. Sure enough, disabling RRAS solved the problem. (The ultimate answer seems to be that a patch broke my RRAS-based VPN servers and leaked over to the IP stack somehow.) Without the clarification of a Netmon trace, I'd have spent hours trying to eliminate possible culprits.

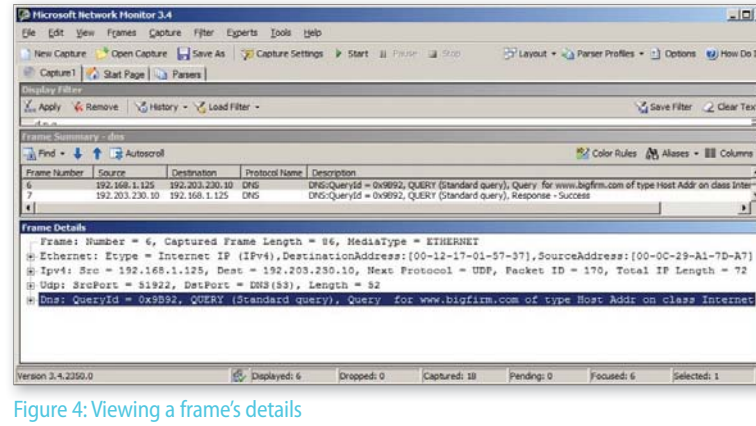


Figure 4: Viewing a frame's details

Dump Nslookup, Get DIG

The basic DNS troubleshooting tool shipped with Windows is of course Nslookup. But did you know that UNIX folks have had a much better alternative for years—Domain Information Groper? DIG isn't built into Windows, but it's easy to find and is a great addition to your DNS toolbelt.

To get DIG, go to the Internet Systems Consortium's Downloads site, at www.isc.org/downloads, and download the latest version of BIND (currently BIND 9.7.2-P3). BIND is a free program that's the Internet's most popular DNS server.

Next, create a folder on your system's hard drive, add the folder to your system's PATH environment variable, and copy the files from the BIND zip file to the folder. (If you prefer, you can delete everything in the folder except the DLL files, dig.exe, and dig.html, which is DIG's Help file—because we're not running BIND, so we don't need all the extra files.)

DIG's basic syntax looks like

```
dig record-to-query-for [@dnsserver]
  [querytype] [+option1, +option2…]
```

So a query such as

```
dig bigfirm.com ns @192.168.1.125
```

would instruct DIG to ask the DNS server at 192.168.1.125 to find all the name server

Figure 5: Expanded DNS frame

records for bigfirm.com. Figure 6 shows this query's output; note the greater level of detail in DIG's output than in Nslookup's.

Skip down a few lines to the two lines that begin with ->>HEADER<<-; you can see the DNS header information basically taken from the frame and reformatted a bit. The *status* info tells you whether the query failed because the record doesn't exist (NXDOMAIN), there was some sort of configuration error on the server (SERVFAIL), no error at all (NOERROR), or an invalid query, such as asking for a record type that doesn't exist (FORERR).

You then see the flags in the DNS header. A nice feature of DIG is that it lets you force the DNS header flags to particular values when you make your query. So, for example, if you were to add +norecurse, DIG would set the flag telling the DNS server in question to perform only the first step in resolving bigfirm.com, which in this case would return only the root servers.

The option +trace takes things a step further and causes DIG to print out exactly what the DNS server is doing as it finds bigfirm.com's DNS server. This tool is very useful for anyone running AD, because security forces us to run our AD-serving DNS hierarchies outside of the public hierarchy, which can lead to a number of configuration errors that +trace can help smoke out. Put DIG on a USB stick and run it on a troubled system with +trace to find the domain controller's (DC's) host record; this action will often shed some light on the problem. Once you give DIG a try, I bet you'll never go back to Nslookup.

Check EDNS

Let's finish with a topic that I keep running across and am constantly asked about. I've found that people seem to think that a DNS feature called EDNS is making Server 2008 R2–based DNS servers incapable of resolving common Internet domain names and that the solution is to disable EDNS—in truth, EDNS isn't new, nor is it at fault. Like many bedrock Internet protocols, our requirements for DNS have outgrown their original 1983 (RFC 882) specifications, forcing the Internet authorities to try to figure out how to shoehorn new capabilities into a small and inflexibly laid-out space.

I say that DNS is inflexibly laid out because it relies heavily upon a small number of 1-bit flags that indicate such things as whether a query needs recursion and whether a given DNS server is capable of a recursive search. The original RFCs allow only enough space for seven such flags, of which only one remains unused. Got a great idea to solve a DNS problem with a useful new flag? Too bad, unless something changes—there's no room at the inn.

The small-space issue stems from the fact that whenever DNS communicates via UDP—which is preferable, because UDP is so fast and the Internet contains so much DNS traffic—it's constrained to a maximum packet size of 512 bytes. That 512-byte maximum was mandated by RFCs 883 (1983) and 1035 (1987) and is based on 1980s network realities that no longer apply. For example, have you ever noticed that very few domains on the Internet have more than 13 DNS servers? Even the massively overworked root domain advertises 13 DNS servers, even though it actually hosts 236 servers and uses clustering to make so many appear to be so few. This is because advertising more than 13 servers would create a packet that's larger than 512 bytes, thus forcing a fallback to the much-slower TCP.

So we needed more flags and bigger packets, but we didn't want to expand DNS in a way that would create a worldwide DNS compatibility nightmare in the process. The answer? 1999's RFC 2671 and EDNS. EDNS provides a clever way for an ever-growing population of EDNS-aware DNS servers to detect whether they're talking to fellow EDNS-aware servers (and thus enjoy the benefits of more flags and more space), or instead are speaking to EDNS-deaf servers (in which case they remain within the pre–RFC 2671 realities, thus avoiding compatibility issues).

When an EDNS-aware requestor queries a responder for a DNS record, it formats the request in standard DNS format but then adds an extra record to its request: a new-to-EDNS kind of DNS record called an OPT record. OPT isn't like the more familiar DNS records, such as A, MX, NS, SOA, and CNAME; you'll never see an OPT record in a zone file. It's more like a secret handshake that only EDNS-aware servers know—a bit of data added to a query.

For example, suppose an EDNS-aware requestor wants to retrieve the A record for a system named PC1 in the bigfirm.com zone from bigfirm's DNS server. A pre-EDNS requestor would just request the A record of the responder. In contrast, an EDNS-aware requestor would say, "I've got two requests for you: First, I need the A record for 'PC1' in bigfirm.com, and second, here's an OPT query with the value '4000.'" The 4000 value is the requestor's way of saying, "Hey, I understand EDNS and if you want to send me a packet that's larger than 512 bytes, I can handle any UDP packet up to 4,000 bytes." If the responder isn't EDNS-aware, it won't recognize the OPT record—and in that case just ignores

```
C:\>dig bigfirm.com ns @192.168.1.125

; <<>> DiG 9.7.2-P2 <<>> bigfirm.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39327
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;bigfirm.com.            IN    NS

;; ANSWER SECTION:
bigfirm.com.        3600  IN    NS    netdoor.minasi.com.
bigfirm.com.        3600  IN    NS    web2.minasi.com.

;; ADDITIONAL SECTION:
web2.minasi.com.    3151  IN    A     70.165.73.5

;; Query time: 77 msec
;; SERVER: 24.178.162.3#53(24.178.162.3)
;; WHEN: Fri Nov 12 12:59:53 2010
;; MSG SIZE  rcvd: 93
```

Figure 6: Output of DIG query

it, responding only to the familiar A record query type and emitting no error messages (and thus preserving backward compatibility). But if the responder is EDNS-aware, it responds to both the A record request and the OPT request; in the OPT response, it also includes a number declaring how large a UDP packet *it* can handle. Thus, if a requestor were to send an OPT=4096 query at the end of another query, and if the responder came back with an OPT=1280 response, then the requestor would know first that the other side understood EDNS and second that it can use oversized UDP packets, but no larger than 1,280 bytes.

So, how does this process go wrong? Well, imagine that your EDNS-aware Server 2008 R2 server queries another EDNS-aware server, and they decide to use a UDP packet that's larger than 512 bytes. This size of packet can become fragmented (whereas 512-byte packets almost never do), and many cheap Network Address Translation (NAT) routers discard fragmented packets. Worse yet, some firewalls have security rules that say, "If it's DNS and UDP and it's bigger than 512 bytes, it must be evil—discard it." In either case, the result is the same: a failed resolution.

The best solution is to figure out what hop on the journey caused the problem, but that's not always possible. Another approach is to simply tell your Server 2008 R2 server to no longer send out OPT queries, and thus to never initiate EDNS transactions. You can do that from an elevated command prompt with the following command:

```
dnscmd /config /enableednsprobes 0
```

No reboot is necessary after this command, and replacing the 0 with a 1 undoes the effect. However, the only effect of this command is to prevent Server 2008 R2 from starting an EDNS conversation. If a DNS server queries the Server 2008 R2 server with an OPT packet, the Server 2008 R2 server will happily respond in EDNS fashion—so make sure that your routers and firewalls don't have an outgoing filter that kills big DNS UDP packets!

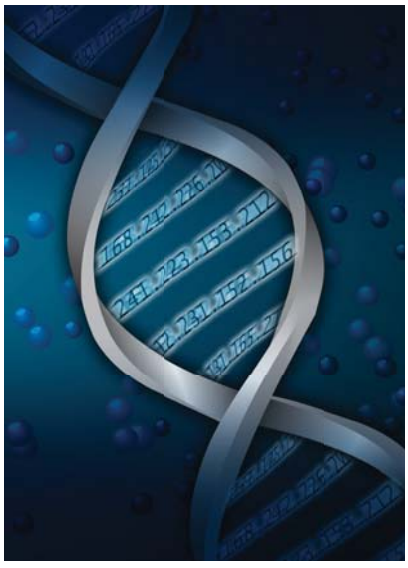
EDNS isn't new to Windows Server; Windows DNS has supported it since Server 2003. Server 2008 R2's only change was to enable the probes. Nor is EDNS some sort of exotic futuristic protocol; rather, some sniffing of my Internet traffic shows that at least 85 percent of DNS servers of all stripes understand EDNS and are using it to good advantage. It would be a shame to make your Server 2008 R2 DNS server miss out on EDNS's advantages, so you should do a bit of router reconfiguration before deprobing your DNS server.

Plan Ahead

DNS failures are big problems, but they're easily conquered with a bit of housekeeping, keeping up on the best tools, and staying abreast of what's new in DNS. Try out some of what you've learned here, and you'll be better prepared to fix the really bad stuff!

InstantDoc ID 129166

Mark Minasi
(www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books.



DNS in Windows Server 2008 R2

A more complex AD design means a more complicated DNS structure

by Russell Smith

DNS, which is responsible for resolving domain names to IP addresses, isn't just the name resolution system that underpins the global Internet—it's also a critical component in Active Directory (AD) for locating network resources. But despite the ubiquitous nature of DNS in Windows networking over the past decade as a replacement for Microsoft's proprietary WINS, DNS is a complex hierarchical system that many junior administrators find difficult to grasp.

In this article, we'll look beyond a single-forest/single-domain AD structure, where DNS configuration is relatively straightforward, and investigate how DNS works in a more complex AD design. Along the way, we'll introduce some of the new DNS concepts in Windows Server 2008 R2.

Active Directory and DNS Integration

To help us understand how DNS integrates with AD, let's configure an AD structure that's commonly deployed in midsized and large organizations. We'll create a single forest with two domains, as Figure 1 shows. The first domain will be what's often referred to as an *empty root,* or just *root,* domain. An empty root domain sits at the top of the AD hierarchy and, as its name suggests, doesn't contain any resources. This type of domain gives organizations more flexibility and better separation of security roles than a single forest/single domain. The second domain will sit below our empty root and is therefore a child domain; it will function as the main domain for our organization, where resources (e.g., groups, user and computer accounts) are located.

We start by running Dcpromo on the first server to create the forest and empty root domain. Log on to Server 2008 R2 as an administrator. Make sure that you've given the server an appropriate name, such as DC1, and set an IP address, subnet mask, and default gateway on the server's NIC. You can leave the NIC's DNS settings empty and let Windows add a local address.

Run Dcpromo from the Start menu and create a new forest and domain called ADcompany.com. Note that I appended AD as a prefix to the company name to keep the internal and external DNS namespaces separate. ADCOMPANY will become the NETBIOS name for the domain. Even though the domain is intended for internal use only, it's important to register the ADcompany.com domain on the Internet to ensure that clients can't be accidentally redirected to a device that's outside the organization's control. It's also common to use the AD.company.com namespace hierarchy, where AD becomes the NETBIOS name for the domain. In this case, assuming company.com is already registered by the company on the Internet, no additional action is required.

On the Additional Domain Controller Options screen, make sure the *DNS server* option is selected. After you click Next and Dcpromo begins to validate the selected options, you'll receive a warning stating that a delegation can't be created because the authoritative parent zone can't be found. In other words, Dcpromo can't find an authoritative DNS server (i.e., a server that holds a primary or

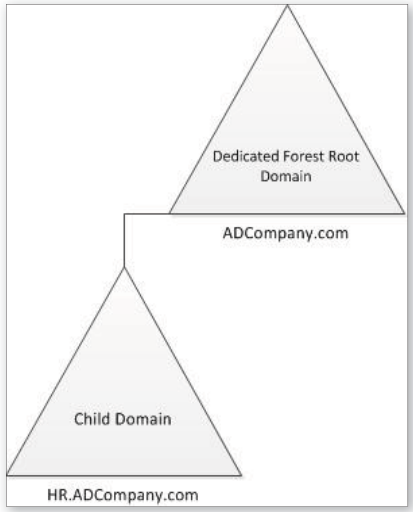


Figure 1: Single forest with two domains

secondary copy of zone data for the .com domain), where it can create a delegation zone for the ADcompany.com domain.

A DNS zone holds all resource records for one part of the namespace, such as ADCOMPANY or COM. Because this is our internal root AD domain, a delegation record in the public COM zone isn't necessary and you can ignore this warning. We'll understand more clearly what delegation means when we create our child domain.

Testing with Dcdiag

After Dcpromo finishes, reboot the server as prompted. To make sure that everything is working as expected with our new domain, open a command prompt and run Dcdiag. A series of tests will be carried out that should pass with success if DNS and other critical AD components are configured correctly.

Before running Dcdiag, you might want to clear the System and DFS Replication event logs to prevent the tool from reporting various failures because of error warnings logged during the domain setup process. For example, DFS replication errors are typically shown when Dcdiag is run for the first time on a new domain controller (DC)—however, they don't necessarily indicate a problem with DNS, which is often the source of replication failures. After the event logs are cleared, run

```
dcdiag /test:dfsrevent
```

The test should be a success.

Until you configure a time source, you'll get W32tm (Windows Time service) errors in the Dcdiag tests for the root domain's DC. For information about configuring the Windows Time service, see the Microsoft article "How to configure an authoritative time server in Windows Server" at support.microsoft.com/kb/816042.

Root Hints

Now that AD DNS is working, if the DC has a connection to the Internet, the installed DNS server should let us resolve Internet domain names even though we haven't configured any forwarders or added an IP address for an ISP's DNS server on the DC's NIC settings. The DNS server includes root hints that point to the top-level DNS servers on the Internet so that it can resolve queries for names that it isn't authoritative for and doesn't already have in its cache.

To see the root hints loaded from the cache.dns file, open DNS from Administrative Tools on the Start menu. In the DNS console, right-click the DNS server in the left pane and select Properties. In the server properties dialog box, select the Root Hints tab, as Figure 2 shows.

You might encounter situations, such as the requirement to use OpenDNS for web content filtering, in which you set up a forwarder for Internet name resolution instead of relying on root hints. When designing your DNS infrastructure, remember that if forwarders are configured on a DNS server, they're used for name resolution before root hints.

Iterative and Recursive Queries

Requests made by the DNS server to resolve names using root hints are iterative, meaning that a best answer will be accepted—which might be a referral to a name server lower down the hierarchy that can resolve the query definitively. This is in contrast to the Windows DNS client, which sends recursive queries to a DNS server, requiring a definitive answer or an error stating that the resource doesn't exist. Recursive queries are typically sent by DNS clients or forwarders.

Configuring a Child Domain

Now that internal and Internet name resolution have been tested and are working in our root domain, it's time to add a child domain, called HR (HR.ADcompany.com), where all our resources will be located. Log on to the second Server 2008 R2 machine as a local administrator and make sure it has an appropriate name, such as DC2. Assign an IP address and subnet mask, then set the primary DNS server for the server's NIC with the IP address of your DC in the root domain. When we run Dcpromo, the tool needs to locate the root DNS domain and DC, so a DNS server that can answer those queries must be configured.

Before starting, we can run

```
dcdiag /test:dcpromo /dnsdomain:HR
  .ADcompany.com /ChildDomain
```

to ensure that everything is configured properly for Dcpromo to promote this server to a DC for the domain specified using the /dnsdomain switch.

Now run Dcpromo from the Start menu, this time opting to create a new domain in an existing forest. On the Network Credentials screen, enter the forest domain (ADcompany.com) and an account that's a member of the Enterprise Administrators group in the root domain, as Figure 3 shows. In the *Name the New Domain* dialog box, enter the

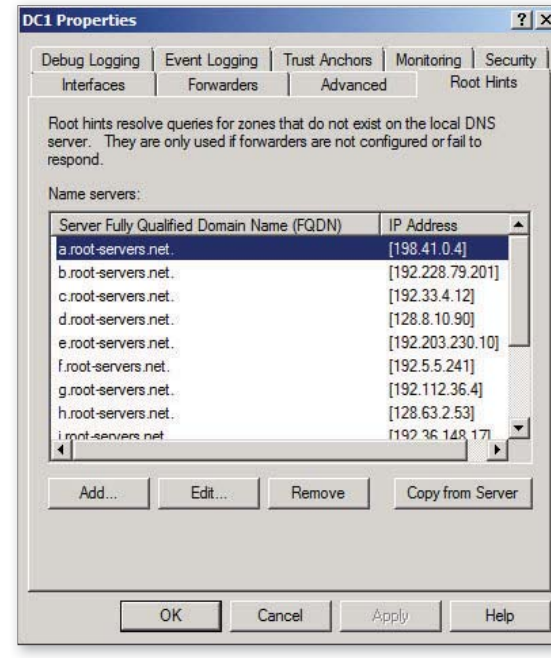


Figure 2: Viewing root hints

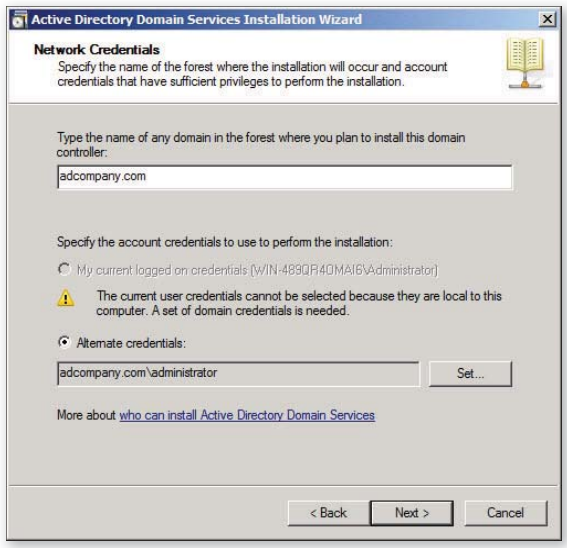


Figure 3: Creating a new domain in an existing forest

Fully Qualified Domain Name (FQDN) for the root domain (ADcompany .com) and single-label name for the new child domain (HR), as Figure 4 shows. In the Additional Domain Controller Options dialog box, select *DNS server.* For the rest of the wizard, accept the default settings.

Reboot the server when prompted, and run Dcdiag on the HR DC to ensure that everything's working as expected, following my earlier advice for running Dcdiag. Open a command prompt and run

```
ipconfig /all
```

Note that the server's NIC primary DNS is set to the local server address, and the root domain's DNS server IP address is shifted to act as a secondary DNS server.

Delegation and Forwarding

Still working from the command prompt, make sure that you can ping the DC in the root domain, using either the DC's single-label name (DC1) or FQDN (DC1 .ADcompany.com). You should also be able to ping an Internet domain name from the child domain's DC, assuming it has Internet connectivity. From the root domain's DC, make sure that you can ping the DC in the child domain. The DNS server in the child domain refers queries for resources in ADcompany .com to a forwarder, which is automatically configured when Dcpromo runs. To see this configuration, open the DNS server console on the child domain's DC from Administrative Tools on the Start menu. In the DNS console, right-click the server in the left pane and select Properties. In the properties dialog box, select the Forwarders tab; you'll see that the server is configured to send all queries that it can't resolve to the root domain's DNS server. Both internal and Internet queries are forwarded; this is different from a conditional forwarder, which is configured to forward queries that can't be resolved locally only for a specific namespace.

Conversely, on the root domain's DNS server you'll find a delegation record (sometimes referred to as a delegation zone) for the HR domain. Again, this record was configured as part of the Dcpromo process for the child domain's DC and lets the root domain's DC locate resources in the child domain. Open the DNS console on the root domain's DC; in the left pane, expand DNS Server, Forward Lookup Zones, ADCompany.com. Click the HR delegation zone at the bottom of the tree. In the right pane you'll see a host (A) record for the child domain's DNS server. Delegation and forwarding are the default mechanisms in Windows Server for enabling resolution up and down a branch of a contiguous DNS namespace, as Figure 5 shows.

DNS Devolution

DNS devolution is a feature of the Windows DNS client. It isn't new to Server 2008 R2 or Windows 7, but it offers added security. From the child domain's DC, we can ping resources in the root domain without specifying the FQDN (i.e., we can ping DC1 without having to enter DC1.ADcompany.com). The same is true from the root domain's DC; we can ping DC2 successfully without the FQDN.

By default, devolution attempts to resolve a single-label name by appending domains from the client's Primary DNS Suffix (PDS). So a machine that belongs to the AD.contoso.com domain will first try to resolve a machine name as DC1 .AD.contoso.com and then DC1.contoso .com. It won't try to resolve DC1.com because the default devolution level is 2, which is the default setting in Windows prior to Server 2008 R2 and Windows 7. In some situations, a default level of 2 can create a security concern if DNS clients try to resolve FQDNs that are outside the control of the organization. For example, consider the following set of queries when the devolution level is set to 2: DC1.HR.company .co.us, DC1.company.co.us, DC1.co.us. The final query, DC1.co.us, is outside the organization's control and could result in a client accidently connecting to a malicious machine on the Internet.

In Server 2008 R2 and Windows 7, the default behavior is to set the devolution level to the number of labels in the Forest Root Domain (FRD) if the PDS ends with the FRD. Our PDS is HR.ADcompany .com and our FRD is ADcompany.com—so according to the default behavior in Server 2008 R2 and Windows 7, devolution is enabled and the level is set to 2 for our DNS clients. Microsoft issued an update to change the DNS devolution behavior in Windows Vista, Windows XP, and Windows 2000. For more information about the update, see the Microsoft article "Post-installation behavior on client computers

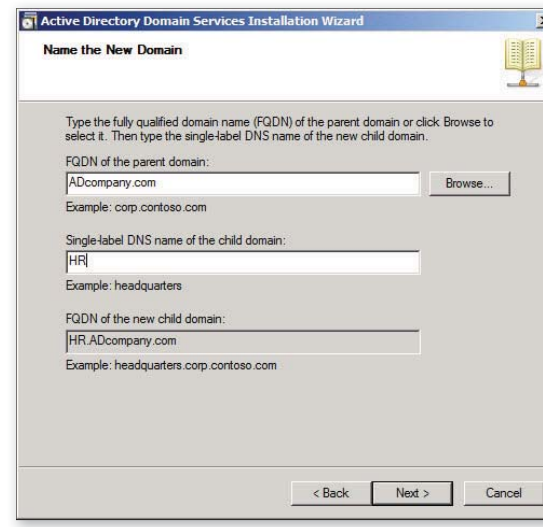


Figure 4: Naming the new domain

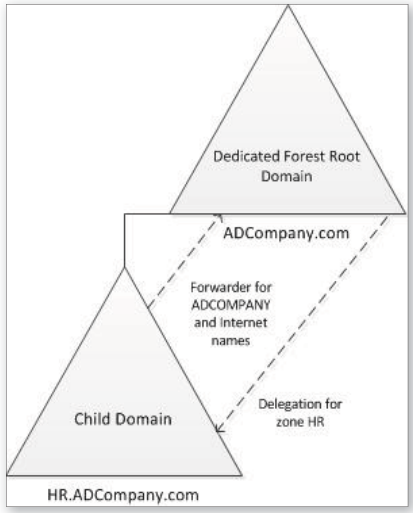


Figure 5: Delegation and forwarding

after you install the DNS update" at support.microsoft.com/kb/957579.

DNS Suffix Search List

If we add a third domain to our forest, finance.ADcompany.com, DNS devolution might not be enough to resolve single-label names of resources in HR.ADcompany.com from clients in the FINANCE domain. Single-label name resolution works from the FINANCE domain if you try to ping resources in the HR domain when all devices are located on the same physical subnet. This is because Windows will broadcast for the IP address if it can't successfully resolve the name from the machine's local cache or configured DNS server.

If you use Nslookup to test DNS resolution, you'll see that without a DNS suffix search list, you must enter the FQDN of the resource located in the HR domain, because as a tool for testing DNS name resolution, Nslookup uses DNS exclusively. To test DNS with Nslookup, open a command prompt from the Start menu, type

```
nslookup
```

At the prompt, enter the FQDN or single-label name that you want to resolve and press Enter. Nslookup will return the IP address or report a lookup failure.

If resolving single-label names across all AD domains is important to you, you can configure the DNS suffix search list on all devices with a list of primary DNS suffixes that you want to resolve (e.g., finance.ADcompany.com, HR.ADcompany.com, and ADcompany.com). If a DNS suffix search list is configured for a DNS client, DNS devolution is automatically disabled. A search list can be configured manually (select *Change adapter settings* in Windows 7's Network and Sharing Center) for each NIC on the DNS tab in the Advanced TCP/IP Settings dialog box for the IPv6 and IPv4 properties. Alternatively, a search list can be configured using a comma-delimited list in the DNS Suffix Search List setting under Computer Configuration, Policies, Administrative Templates, Network, DNS Client in Group Policy (for Windows Server 2003 and XP or later).

Similarly, if we add a new DNS zone, secure.HR.ADcompany.com, on the HR DNS server for the purposes of creating a separate zone for important server resource records that should be secured with DNS Security Extensions (DNSSEC), we need to deploy a DNS suffix search list so that DNS clients can locate resources in the new zone by single-label name. A new DNS zone is required in this case, because DNSSEC doesn't support dynamic updates—the ability of client host records to automatically update on a DNS server—which is the default and desired setting for DNS zones where host records are stored for client computers. Typically, IP addresses of server computers don't change, so secured zones can be manually administered.

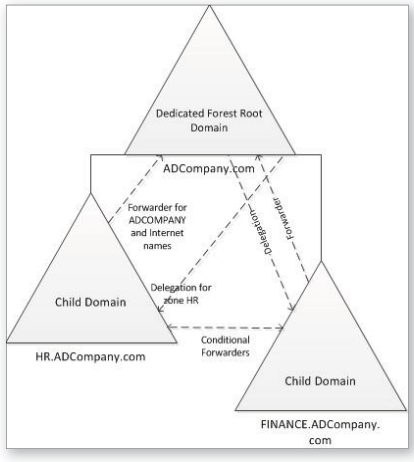


Figure 6: Conditional forwarding

Conditional Forwarding

We can help our two child domains, finance.ADcompany.com and HR.ADcompany.com, resolve cross-domain queries more efficiently, without the need to send a recursive query to the DNS server in the forest root, by configuring a conditional forwarder on the DNS servers in both child domains. Conditional forwarders take priority over server-level forwarders and are more efficient in that we can set queries for specific domain suffix(es) to be sent to a predefined DNS server, as Figure 6 shows.

The DNS server in HR.ADcompany.com will contain a forwarder that sends all queries for finance.ADcompany.com to the primary DNS server for the FINANCE domain, and vice versa. To configure a conditional forwarder, open the DNS console on the DC in the HR domain from Administrative Tools on the Start menu. In the left pane of the DNS console, expand the DNS server, right-click Conditional Forwarders, and select New Conditional Forwarder from the menu. In the New Conditional Forwarder dialog box, enter finance.adcompany.com in the DNS Domain box. Under *IP addresses of the master servers,* enter the IP address or server name of the DNS server in the FINANCE domain, and press Enter. Click OK, then repeat the process on the DNS server in the FINANCE domain, but enter HR.ADcompany.com in the DNS Domain box and the IP address of the DNS server in the HR domain.

DNS Complexities

I can't cover all bases in one article—for example, there are two additional zone types, secondary and stub zones, that you can use to improve performance, as well as new Server 2008 R2 features, such as DNSSEC. But a basic understanding of how DNS and AD work together as an integrated solution will help you design new AD deployments and troubleshoot any problems. Most important, when testing a new or existing AD infrastructure, make sure that for each domain you can ping resources in all other trusted domains. In addition, deploy delegation and conditional forwarding to enable resolution between namespaces. These basics will help you use DNS more effectively in complex AD environments.

InstantDoc ID 129442

Russell Smith
(rms45@rsitc.com) is an independent IT consultant specializing in systems management and security, and author of *Least Privilege Security for Windows 7, Vista and XP* (Packt).

Exchange Server 2010 SP1 Mailbox Import and Export

A new beginning

by Tony Redmond

Microsoft has always had a blind spot when it comes to getting data into or out of Exchange Server. Applications that include persistent data repositories typically provide a mechanism to let administrators load data into or export data out of the repository—but not for Exchange. Data import mechanisms are used to load user data into mailboxes, often during a migration from another email system, whereas data export mechanisms are used for the reverse purpose, usually to extract data for later examination, in scenarios such as legal discovery when companies need to provide copies of messages and attachments for legal review.

Over the past 15 years, since Microsoft first released Exchange, administrators have had to resort to client-side tools to load or export data from mailboxes. In some cases these tools have been highly functional. The ExMerge utility (msexchangeteam.com/archive/2004/07/01/171051.aspx) is a good example; this tool began as a solution created to help customers move mailbox data into Exchange from other email systems and evolved into an essential part of an Exchange administrator's arsenal. Outlook is the most common mechanism used to access mailbox data. Outlook is an adequate solution for quickly browsing a mailbox to extract items to a PST file, but it's not designed to import gigabytes of data—nor is it scriptable or programmable by the average administrator who simply wants to extract user data to satisfy a request for information. Skilled programmers can use the Outlook Object Model (OOM) to extract data, but the necessary code often isn't available when you need it. Thus many administrators resort to programs such as ExMerge.

Client applications depend on MAPI libraries to access the contents of Exchange databases. The most accessible MAPI libraries in terms of documented APIs are those provided with Outlook. You must therefore install Outlook on an Exchange server before you can run a client that depends on the MAPI libraries. This dependency also exists for Exchange Server 2010's and Exchange Server 2007's Import-Mailbox and Export-Mailbox cmdlets. When Microsoft released Exchange 2010 in October 2009, you had to install a 64-bit version of Outlook on your Exchange 2010 mailbox servers before you could run the cmdlets to import or export data. However, the 64-bit version of Outlook wasn't formally released until Outlook 2010 came along in April 2010—which illustrates the problems that occur when one product depends on another but development schedules aren't aligned. In reality, Exchange's import/export capability was a mess for years and in dire need of a redesign.

Exchange 2010 SP1 discards previous import/export approaches in favor of a new model based on import and export requests managed by the Microsoft Exchange Mailbox Replication Service (MRS). Data moves into and out of Exchange via a new data provider that's integrated into the Client Access server role and isn't dependent on any other product. The old Import-Mailbox and Export-Mailbox cmdlets are eliminated in SP1, which means that you must rewrite any PowerShell scripts to automate data loads or extracts that depend on the cmdlets. A new set of cmdlets exist in SP1 to create mailbox

import and export requests, retrieve their status, report their disposition, and so on. This new mailbox import/export approach is similar to Exchange 2010's mailbox move model.

Preparing for Import and Export Operations

Before we look at the details of the new cmdlets and explore some examples, let's examine the prerequisites. First, administrators can't import or export mailbox data unless they have explicit permission to do so. This restriction is to protect the integrity of user mailboxes because you obviously don't want every administrator to be able to manipulate user data. The ideal situation is to restrict access to a limited set of administrators and to audit access regularly. Access is gained through membership in the Role Based Access Control (RBAC) Mailbox Import Export role group. Users who are members of this group can run the new cmdlets, whereas users who aren't members of the group won't be able to queue mailbox import or export requests. In fact, they won't even be able to run the cmdlets. Exchange won't load the cmdlets into these users' Exchange Management Shell (EMS) session because their accounts aren't members of the Mailbox Import Export role group.

Second, all data is imported from PSTs and exported to PSTs. No other data format is supported—which shouldn't be an issue, because the PST format is the de facto standard for moving data into and out of Exchange. Output PSTs created by Exchange use the latest Unicode format. Exchange can import data from PSTs in both Unicode and the older ANSI format. Data can be imported from a PST into several different mailboxes, but only a single mailbox import request can access a specific PST at a time. No other client can access a PST while Exchange is using it.

Third, PST files that contain data to be imported into mailboxes must be placed in a file share that allows read/write access for the Exchange Trusted Subsystem group, as Figure 1 shows. Exchange 2010 uses the Exchange Trusted Subsystem group to let Exchange servers access secure data. You don't need to grant any other access to the file share. Likewise, when Exchange exports data out to a PST, it writes the PST into a secured file share. The reason Exchange uses a file share is simple: All mailbox processing is performed by the MRS running on the Client Access server. It's possible to assign a mailbox import or export request for processing by a specific MRS instance—but if you don't, any MRS instance running on the Client Access server can process the request. Thus you can't assume that the MRS instance will run on the same server on which the data to be imported is located. The data location must be accessible to any Client Access server in the site—hence Microsoft's decision to use a file share.

> Data moves into and out of Exchange via a new data provider that's integrated into the Client Access server role.

Although Microsoft did a nice job of introducing the new import/export model in Exchange 2010 SP1, the nature of software development is such that the first version can't address everything. In this case, you have to run all mailbox imports and exports through EMS because Microsoft wasn't able to upgrade the previous mailbox import and export wizards that are available in the Exchange 2010 version of Exchange Management Console (EMC). Forcing administrators to use EMS isn't a great hardship, and it's certainly a good tradeoff to be able to use the new model's increased level of functionality, as well as drop the silly requirement to install Outlook on an Exchange server before you can access mailbox data.

Table 1 lists the new cmdlets that Exchange 2010 SP1 provides to import and export mailbox data. The older Import-Mailbox and Export-Mailbox cmdlets are no longer available in SP1.

The Exchange 2010 SP1 Help file contains many useful examples of how to use the new cmdlets, including the format required by the different parameters. The new cmdlets' wide range of functionality gives third-party developers and consultants wide scope for building future tools to automate mailbox imports.

Importing Mailbox Data

Let's explore how the cmdlets are used to import mailbox data. First, we create a new mailbox import request, like so:

```
New-MailboxImportRequest -Mailbox
  'TRedmond' -FilePath '\\ExServer1\
  Imports\TRedmond.pst' -Name
  'Import-TR' -ConflictResolutionOption
  KeepLatestItem -BadItemLimit 5
```

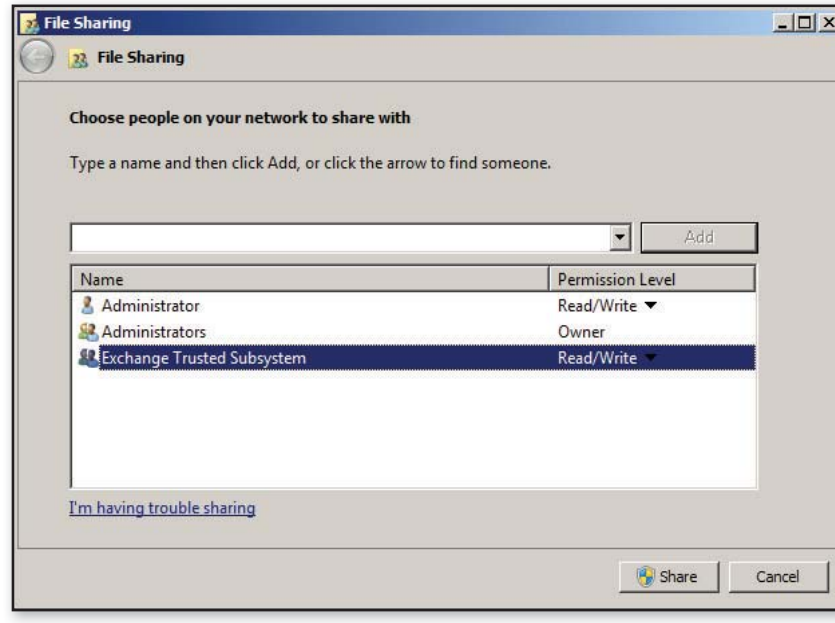


Figure 1: Allowing read/write access for the Exchange Trusted Subsystem group

Table 1: Exchange 2010 SP1's Mailbox Import/Export Cmdlets

Cmdlet	Use
New-MailboxImportRequest	Create a new mailbox import request for processing by the MRS
Set-MailboxImportRequest	Set properties of a mailbox import request
Get-MailboxImportRequest	Retrieve the current status of a mailbox import request
Remove-MailboxImportRequest	Remove a mailbox import request
Get-MailboxImportRequestStatistics	Report detailed information about a mailbox import request
Suspend-MailboxImportRequest	Suspend an import operation from a PST
Resume-MailboxImportRequest	Resume a suspended import operation
New-MailboxExportRequest	Create a new mailbox export request
Set-MailboxExportRequest	Set the properties of a mailbox export request
Get-MailboxExportRequest	Retrieve the current status of a mailbox export request
Get-MailboxExportRequestStatistics	Report detailed information about a mailbox export request
Remove-MailboxExportRequest	Remove a mailbox export request
Suspend-MailboxExportRequest	Suspend an export operation to a PST
Resume-MailboxExportRequest	Resume a suspended export operation

This command creates a new import request for the mailbox with the alias TRedmond and identifies that the source PST file is located on a file share called Imports on a server called ExServer1. After it's created, the import request is held in an Active Directory (AD) queue. The request will be processed by the first MRS instance in the site to become aware of the request.

By default, Exchange checks for duplicate items when it imports data into a mailbox; it doesn't create a copy of an item if it already exists in the target mailbox (the message identifier is used to detect duplicates). In this case, the ConfictResolutionOption parameter specifies that if a duplicate is detected during import, Exchange should keep the latest version of the item. The other options are KeepAll (keep all versions) and KeepSourceItem (keep the version of the item from the import PST).

In the example code, a unique name called Import-TR is provided for the import request. This parameter is optional; if you don't provide a name, Exchange will use the default MailboxImport. If you create multiple import requests for the same mailbox, Exchange will use names such as MailboxImport1, MailboxImport2, MailboxImport3, and so on to uniquely identify each import operation. The mailbox name and the request name are combined and used to retrieve information about the import request.

Assigning a specific name to an import request becomes important if you want to run multiple concurrent imports for the same mailbox, each of which processes data from a different PST. (You can't run concurrent imports from the same PST.) In this scenario, the default names assigned by Exchange work perfectly well, but it's easier to track each job's progress and troubleshoot errors if you assign more meaningful names, such as the name of the source PST.

You don't have to import everything in a PST because the ExcludeFolders and IncludeFolders parameters let you control exactly which folders Exchange imports. For example, to import just a few named folders, we can pass their names as follows:

```
-IncludeFolders "Project Bingo",
  "My Important Stuff", "Personal
  Information"
```

If you wanted to include all the folders under a specific root folder, you'd pass the name of the root folder as follows:

```
-IncludeFolders "Projects/*"
```

In this example, all the data in the subfolders under the Projects folder will be imported. If you need to navigate to a specific folder deep in the hierarchy, you can pass its name like so:

```
-IncludeFolders "Projects/2010/Great
  Wall of China"
```

PSTs often contain *associated items,* which are hidden items used by Outlook to store data such as rules, forms, and views. Exchange doesn't import associated items unless you configure it to do so by setting the AssociatedMessagesCopyOption parameter to Copy. In most cases, you can avoid copying associated items from a PST because an equivalent associated item is likely to already exist in the mailbox. An exception would be if an application required forms that you knew didn't already exist in the mailbox.

After you submit a job and the MRS starts to process it, you can retrieve progress information. In our sample scenario, we'd use the Get-MailboxImportRequest cmdlet, as follows:

```
Get-MailboxImportRequest -Identity
  'TRedmond\Import-TR'
```

Note that the name of the mailbox (TRedmond) and the request (Import-TR) are combined to form a unique identity for the job we're interested in.

The Get-MailboxImportRequest cmdlet supports several parameters to let you retrieve the status of different groups of jobs.

- The BatchName parameter fetches details of all requests that belong to a specific named batch.
- The Database parameter fetches details of all requests that belong to mailboxes in a specified mailbox database.
- The Status parameter fetches details of all requests with a specified status. Valid status codes include Completed, InProgress, Queued, CompletedWithWarning, Suspended, and Failed.

To report the progress of an import, you can use the Get-MailboxImportRequest Statistics cmdlet to discover how much data

Listing 1: Get-MailboxImportRequestStatistics

```
Get-MailboxImportRequestStatistics -Identity 'TRedmond\Import-TR' | Select Name,
  Status, StatusDetail, BytesTransferred, ItemsTransferred, EstimatedTransferItemCount,
  BytesTransferredPerMinute
Name                        : Import-TR
Status                      : InProgress
StatusDetail                : CopyingMessages
BytesTransferred            : 191.6 MB (200,929,681 bytes)
ItemsTransferred            : 2346
EstimatedTransferItemCount  : 4233
BytesTransferredPerMinute   : 75.82 MB (79,505,066 bytes)
```

has been transferred. Initially you'll see that the MRS creates the folder hierarchy in the target mailbox to accept the imported data; then you'll observe an increasing count of transferred items as the MRS moves data from the PST into the mailbox. For example:

```
Get-MailboxImportRequestStatistics
  -Identity 'TRedmond\Import-TR' |
  Format-List
```

The Get-MailboxImportRequestStatistics cmdlet reveals a lot of information. Thus it's a good idea to limit the properties returned, to reveal only essential data about the import operation. I typically use the command that Listing 1 shows. Figure 2 illustrates the New-MailboxImportRequest, Get-MailboxImportRequest, and Get-MailboxImportRequestStatistics cmdlets in action.

When the import finishes, you can use the Get-MailboxImportRequestStatistics cmdlet to retrieve a report of everything the MRS did to populate the mailbox with data from the PST:

```
Get-MailboxImportRequestStatistics
  -Identity 'TRedmond\Import-TR'
  -IncludeReport | Format-List
```

The report is dumped to screen by default. However, piping the output to a text file results in a more convenient report that's easier to read and that contains a lot more information. The mailbox import report is divided into summary information at the beginning of the report, followed by detailed information about the processing of each folder from the source PST into the target mailbox. Important information includes:

- The name of the source PST
- The name of the target mailbox and the database where it's located
- The current status of the job (e.g., completed, with no warnings)
- The number of bad items encountered during processing (three, which is less than the five-item limit specified in the BadItemLimit parameter in the sample command)
- The start and end time for the job and the name of the MRS that processed the job
- The total number of items and their size transferred from the PST into the mailbox
- Whether any folders were explicitly excluded or included

Exporting Mailbox Data

Much the same approach is followed to export data from mailboxes. However, a different set of cmdlets is used. You run the New-MailboxExportRequest cmdlet to create a new export request. For example, to export a complete mailbox to a PST, you might use a command like this one:

```
New-MailboxExportRequest -Mailbox
  'Tony Redmond' -Name 'TRedmond
  Export' -BadItemLimit 5
  -ExcludeDumpster:$True -FilePath
  '\\Ex2010\Exports\TRedmond.PST'
```

This command takes all the content from the nominated mailbox and writes it out to a PST in the file share location. The contents of the dumpster folders are excluded from the operation. If the PST isn't present, Exchange will create a new file; otherwise if you pass the name of an existing PST, the MRS will write the exported data into it.

Experience demonstrates that it's more common to apply qualifiers to filter or restrict the information exported from a mailbox than it is when you import a PST into a mailbox. For example, if you respond to a legal discovery action, you're probably only required to provide copies of specific relevant information rather than a complete dump of a user's mailbox. Exchange uses several parameters to control the data that's exported.

- The SourceRootFolder parameter specifies a folder in the mailbox to use as the base of the export. If this parameter isn't passed, Exchange exports the complete contents of the mailbox. For example, the following command exports only items that are stored in the Project Bluesky folder and any of its subfolders:

```
New-MailboxExportRequest
  -SourceRootFolder 'Projects/
  Project Bluesky' -Mailbox 'TRedmond'
  -FilePath '\\ExServer1\Imports\
  TRedmond.pst' -BadItemLimit 5
```

  In this instance, the Project Bluesky folder is a subfolder of the Projects folder.
- The TargetRootFolder parameter specifies a root folder in the target PST to create the folders exported from the mailbox.
- The IncludeFolders parameter specifies one or more folders that are to be exported. For example:

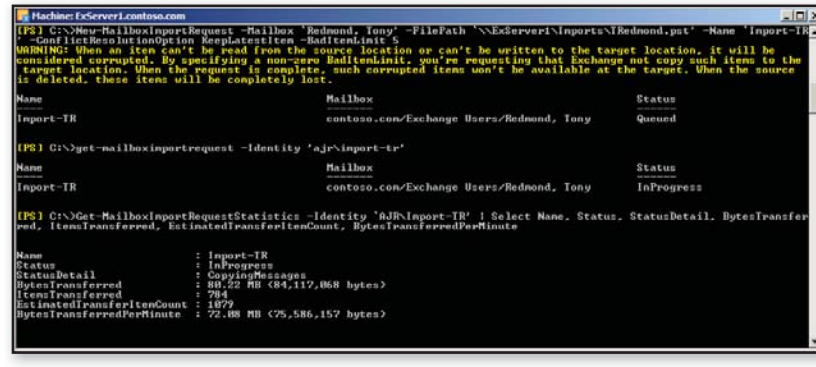


Figure 2: Importing mailbox data with Exchange 2010 SP1

```
New-MailboxExportRequest
  -IncludeFolders 'Projects',
  'Planning/Budgets 2010' -Mailbox
  'TRedmond' -FilePath '\\ExServer1\
  Imports\TRedmond.pst' -BadItemLimit 5
```

- The ExcludeFolders parameter specifies one or more folders that are excluded from the export.
- The IsArchive parameter specifies that the export should be done for the user's personal archive rather than the primary mailbox.

Once again, the Exchange 2010 SP1 Help file contains all the necessary instructions for using these parameters.

Operationally Speaking

During a migration project, you might have to import many gigabytes of information into Exchange. Even with the latest release of Exchange 2010, this isn't a quick task. Some planning is necessary to import information into user mailboxes.

You might need to adjust destination mailbox quotas for the PST data to import. A quota increase might be permanent, or you might be able to adjust it down again after the user has a chance to review the imported material and decide whether it should be kept in the mailbox or moved to an online archive. Increasing the quota for a set of destination mailboxes before an import is a relatively simple procedure to script—but having to adjust quotas is indicative of the manual nature of the processing that PST imports can require.

One way to determine the size of the mailbox quota is by referencing the size of the PST to be imported. Although this approach is reasonably effective, the size of a PST on disk doesn't directly equate to the amount of data that will be imported into the mailbox. The PST file structure imposes a "tax" or overhead of approximately 20 percent over what's required to store items in an online mailbox or archive. You need to ensure that sufficient quota is available in target mailboxes before you begin to import data—or even better, temporarily increase the quota by an excessive amount rather than run the risk that an import will fail because of quota exhaustion.

Optionally, you can import data into archive mailboxes rather than primary user mailboxes. (Use the IsArchive parameter to instruct Exchange to import into the archive.) SP1 lets you place archive mailboxes in databases other than primary mailboxes. You can also use this feature to create databases that are dedicated archive repositories. Remember to check and perhaps adjust archive quotas for target mailboxes before importing data.

Every item that's imported into a mailbox creates a transaction that the Exchange store must capture in a transaction log. I/O demand spikes during the import as the databases that host the target mailboxes commit transactions to accommodate the incoming PST data. Further I/O and CPU activity occurs to add items to the content indexes maintained for the target databases. More I/O is generated if users move information from their primary mailboxes into personal archives after the import operations are complete.

Schedule these operations at times of low user demand.

If the import occurs inside a database availability group (DAG), similar I/O spikes are experienced on servers that host copies of the databases that host target mailboxes because of replication, replay, and indexing activities. This situation has the potential to create a tsunami of I/O activity across the DAG.

The MRS uses the MaxSendSize transport configuration setting to control the maximum size of items it can import into a mailbox. The default size is 10MB. If you want to import larger items, you need to run the Set-TransportConfig cmdlet to increase the setting. For example:

```
Set-TransportConfig -MaxSendSize 20MB
```

Make sure you remove any passwords from the PSTs that you want to import data from because there's no way to provide a password to the cmdlets. Likewise, you can't place a password on a PST when you create it during a mailbox export operation. You must therefore take steps to protect the PST information held in the file share to ensure that the files can't be opened by unauthorized clients. Remember that unlike an OST file that can be opened only when a client has knowledge of the mailbox that owns the replica folders inside the OST, any MAPI client can open a PST file. In addition, the presence of a password on a PST doesn't guarantee its security because many utilities are available on the Internet to crack open a PST in a matter of seconds.

Because Exchange 2010 SP1 is still very new in production environments, it's difficult to characterize how efficiently an individual Exchange server will be able to handle multiple concurrent import or export operations. For this reason it's best to schedule these operations at times of low user demand to avoid competition with the I/O and processing demand created by normal user activity. The ability of an Exchange server to process mailbox data varies from server to server and is highly dependent on current load and system capability. Disk capacity and I/O throughput are obviously important. As an example, importing a 1.35GB PST containing 7,450 items took a server under moderate load 15 minutes to process. Using a more powerful server or scheduling the work to occur at times of low user demand will increase the throughput; most servers should be able to import 8GB per hour.

Look to the Future

You can't underestimate the huge progress Microsoft made by introducing the new mailbox import/export model in Exchange 2010 SP1. A cynic would say that Microsoft merely cleaned up a festering sore that existed in the product since it was first released—and there's some truth in this statement. The history of depending on software such as Outlook and ExMerge certainly isn't one of the high points in Exchange functionality. However, Exchange 2010 SP1 provides such an elegant solution to mailbox import and export that it's pointless to dwell on past limitations.

InstantDoc ID 129031

Tony Redmond
(12knocksinna@gmail.com) is a contributing editor for *Windows IT Pro*, and author of *Microsoft Exchange Server 2010 Inside Out* (Microsoft Press). His blog is available at thoughtsofanidlemind.wordpress.com.

Troubleshooting Active Directory Replication

Keep your domain controller data current to avoid a host of user account problems

by Sean Deuby

One of Active Directory's (AD's) advantages is that it's a distributed application. Its functionality is spread across multiple domain controllers (DCs) so that the failure of any one DC won't affect the overall availability of AD. To accomplish this, AD must move its information around freely and efficiently between its DCs in a process known as replication. The AD replication model is a powerful, fault-tolerant, and complex system. It's also the area that seems to cause the most problems for AD administrators. But that's usually not AD's fault.

Why should you monitor replication and keep it working well? If replication isn't working to one or more of your DCs, a segment of your user population won't be kept current with the latest directory data. This could result in a host of problems: Password changes aren't seen; accounts unlocked by administrators aren't accessible by the account owner; users don't have access to applications (even though they've been added to the correct groups); new users can't log on (even though their accounts have been created); and, very importantly, terminated employees might be able to access the network after their accounts have been disabled.

Replication issues can also affect Group Policy functioning and site or subnet changes. A DC that hasn't successfully replicated with its partner DCs will be tombstoned out of the forest and must be rebuilt. Replication problems can also affect schema updates and have been known to cause forest-wide failures.

The Layered Approach

AD administrators should invest a little time to make sure that AD replication is working correctly for the health of their directory—and of their jobs. As a distributed application, AD depends on all the layers of infrastructure on which it's built. Most of the issues that cause AD service interruptions—including replication—can be traced back to infrastructure or to administrative error (such as accidentally deleting objects). So, the first step in any AD replication troubleshooting must be to make sure that your infrastructure is working correctly. I call this technique troubleshooting from the wire up.

I use the seven-layer OSI network model (physical, data link, network, transport, session, presentation, and application) as a basis for my own AD troubleshooting model. My model is as follows:

- Physical (i.e., the wire)
- Network
- Name resolution
- OS
- Authentication
- The AD application itself

The physical layer refers to the physical network infrastructure: the wires that make networking function. If someone disconnects a network patch cord or runs a backhoe through a fiber circuit, replication isn't going to work.

The network layer refers to network connectivity above the physical layer: router, switch, and, especially, firewall functionality. With regard to firewalls, DCs communicate over so many ports—some dynamically—that it's important to carefully follow the guidance laid out in the Microsoft article "How to configure a firewall for domains and trusts" at support.microsoft.com/kb/179442.

Another network-related issue is remote procedure call (RPC) errors, such as *RPC server is unavailable*. The Ask the Directory Services Team blog includes a very informative post about how to troubleshoot these errors by using the PORTQRY utility. (For more information, see the Microsoft Directory Services Team blog article "Using PORTQRY for troubleshooting" at bit.ly/g5CTuJ.)

Name Resolution: Suspect #1

Name resolution is where you should focus most of your AD troubleshooting efforts because the majority of AD-related problems are caused by name resolution configuration issues. Several years ago, Microsoft Product Support Services traced 80 percent of AD cases to name resolution issues. (For more information, see "Troubleshooting networks without NetMon" at blogs.technet.com/b/askds/archive/2007/12/18/troubleshooting-networks-without-netmon.aspx.)

AD is dependent on DNS to register and resolve all the myriad services and nodes it needs, and there are many ways to configure DNS incorrectly. Microsoft has long recognized this, and the DCPROMO wizard has grown increasingly more sophisticated in the way that it configures DNS. *Windows IT Pro* has published a variety of articles about DNS, including several by Boyd Gerber, a Microsoft network escalation engineer who specializes in DNS. See the Learning Path for a list of *Windows IT Pro* DNS articles. (For more information about how to troubleshoot DNS, see the Microsoft TechNet article "Troubleshooting Active Directory–Related DNS Problems" at tinyurl.com/72ca8h.)

Probably the best command to debug DNS problems is DCDIAG /TEST:DNS. This diagnostic command comprehensively tests the DNS service of a DC or of the server that you direct it to by using the /S switch. Using the /V (verbose) switch provides detailed test results. Adding the /E (enterprise) switch runs the command on all DNS servers in your forest. Finally, you can better analyze the volumes of information that this command provides by piping the output to a file by using the /F switch.

Many of these techniques are covered in the DNS page of my Active Directory Troubleshooting flowchart (deuby.com/adtroubleshooting/ccount/click.php?id=2). You can find additional AD troubleshooting tips on my Active Directory Troubleshooting Tips and Tricks blog at tinyurl.com/adtroubleshooting.

One aspect of AD that's not well known is how name resolution is tied to replication. One of the most common errors we see when replication isn't working is some kind of name resolution error, such as *RPC server is unavailable* or *DNS lookup failure*. Because we humans and most computer services locate other computers on the network by using the DNS A record (e.g., mycomputer.deuby.net), it's natural to assume that this is also how DCs find each other for replication. They do—eventually. But only indirectly. For replication purposes, a DC's directory service registers a GUID in DNS as a CNAME (alias) record. This GUID is unique in the forest. The CNAME is known as the DSA object GUID, and it resolves to the DC's A record. When a directory service on a DC tries to locate its replication partners, it uses the Fully Qualified Domain Name (FQDN) of the CNAME (e.g., 802e2778-27d1-49ca-9d12-5c439f4c4d3b._msdcs.deuby.net).

If you want to find a DC in the same way that another DC really locates one, you have to find its GUID. There are several ways that you can find the DSA object GUID of a DC. One way is to look it up in the Microsoft Management Console (MMC) DNS Management snap-in under the _msdcs container of the domain's zone. However, this method works only if the GUID is registered correctly in DNS. If you aren't sure whether it is, a simple way to verify the registration is to run the command

```
REPADMIN /SHOWREPL <dcname>
```

In this command, dcname represents the name of the DC that's experiencing replication problems. The DSA object GUID is one of the first items listed in the response. Append _msdcs.*domain.com* to the GUID, and that will be what you have to ping.

After you obtain the DSA GUID, ping it from a DC that's receiving the errors. (You could also do this from your own client, but that would probably introduce another variable because you might be using a different DNS server than the one the DC is using.) If you get no response from the ping, or if you receive a "could not find host" error, the replication problem most likely occurs because the CNAME or A record isn't registered correctly. Reregister the DC's GUID and its SRV records either by running the NLTEST /DSREGDNS command or by restarting the NETLOGON service.

Critical Layers: Health and Authentication

The importance of checking the OS health of the DC should be self-evident. AD is an application that runs on top of (or, in the case of Windows Server 2008 R2 or Windows Server 2008, is a role of) the Windows Server OS. There's nothing unique about OS troubleshooting on a DC compared with troubleshooting any other application role. However, a dedicated DC does have an advantage over other application roles if you do encounter OS problems. Instead of spending hours trying to fix an ailing OS, you can simply demote the DC, or forcibly remove the role by using DCPROMO /FORCEREMOVAL. Then, you can quickly rebuild the OS and reinstall AD. This is often the quickest way to get a DC working again.

Similar to name resolution, the authentication layer of the AD troubleshooting model isn't exactly a software layer. It's a vital component within AD that, among

Learning Path

WINDOWS IT PRO RESOURCES:

"Identify and Troubleshoot DNS Problems," InstantDoc ID 125990

"Chasing the DNS Zone Location Problem," InstantDoc ID 104674

"DNS Enhancements in Windows Server 2008 R2," InstantDoc ID 125360

"Deconstructing DNS," InstantDoc ID 48527

"How DNS Works," InstantDoc ID 8666

"A DNS Primer," InstantDoc ID 7733

other functions, determines the valid identities of the DCs themselves to allow them to safely communicate with one another. Kerberos is the security protocol that's used, and the Kerberos Key Distribution Center (KDC) is part of every DC. If you aren't familiar with this protocol (and every AD admin should be), the Microsoft Directory Services Team blog has a helpful article. (For more information, see "Kerberos for the Busy Admin" at bit.ly/egoDj9.)

Kerberos itself is an extremely reliable AD component. With respect to replication between DCs, many authentication-related failures are actually caused by external problems, such as time skew between computers. The W32TM utility is the main tool for correcting time skew, which it does by managing the Windows Time service. For example, you can perform the following actions by running the corresponding W32TM commands:

- Check the last time that your target DC successfully synchronized its time, and with what server: w32tm /query /status
- Force the service to use another DC in the domain: w32tm /config /syncfromflags:DOMHIER
- Force the service to rediscover its network resources, then resynchronize with its time source: w32tm /resync /rediscover

If you've virtualized some of your DCs, make sure that they're not synchronizing time with their host but are synchronizing instead with their partner DCs. (For more information about how to troubleshoot Kerberos, see the Microsoft article "Troubleshooting Kerberos Problems" at technet.microsoft.com/en-us/library/cc786325(WS.10).aspx. For more information about Kerberos troubleshooting by using network traces, even though the cause of the problem is name resolution, see the Microsoft Directory Services Team blog article "Troubleshooting Kerberos Authentication problems—Name resolution issues" at bit.ly/i287M3. The Windows Server 2003 R2 Kerberos Technology Center also provides a range of Kerberos-related articles at bit.ly/9uNVZc.)

How Replication Works

Before you can effectively troubleshoot replication, you must understand how it works. Replication is the process of forwarding updates for a directory partition to all DCs that have a copy of that partition. For example, if you make a change to a user account in the domain child1.mycompany.com, replication forwards that change to the other child1 DCs because those controllers have a copy of (that is, they host) that domain partition. If you make a change to the site configuration for mycompany.com, replication forwards that change to all other DCs in the mycompany.com forest because site information is stored in the configuration partition that's hosted on every DC in the forest. Replication works on a per-partition basis, making replication topology more complicated to understand. The good news is that when replication fails, it usually fails for all partitions on a DC because of issues that affect the supporting infrastructure.

To fine-tune the way that DCs replicate with one another, you create an AD site topology that contains your forest's DCs. The site topology is a network of its own that has sites as its nodes and site links as the connections between the nodes. The topology is usually based on your company's LAN and WAN configuration. You can further tune the way that replication connections are generated between sites by changing the relative cost of the site link (i.e., how expensive the WAN circuit is).

Within a site, each DC uses its Knowledge Consistency Checker (KCC) and its knowledge of the site configuration that's stored in the configuration partition to create connection objects between DCs. Connection objects are the pathways that transmit AD objects and attributes to other DCs (replication partners) via the replication process. These connection objects are one-way pathways. This means that every DC must have at least one inbound connection object to receive updates from each upstream replication partner, and at least one outbound connection object to transmit updates to each downstream partner. Replication from one DC to another is triggered by the upstream DC when it advertises to its replication partners that it has an update to share. The DC advertises this almost immediately (within 15 seconds).

In the same way that DCs are connected within a site, sites are linked to each other for replication by connection objects. But the way that the connection objects are created is controlled by how you set up the site links. Most administrators turn down the site link replication interval to 15 minutes from its default of 180 minutes. If you allowed every DC in every site to replicate with every other DC, the situation would quickly become unmanageable. Therefore, one DC is configured as the bridgehead server for each directory partition in each site. In most cases, one bridgehead server handles intersite replication for all directory partitions.

Both within a site and between sites, replication is a pull operation. In other words, a DC always requests updates from its upstream partners instead of pushing them out to its downstream partners. Therefore, when you troubleshoot, you should always think of objects and attribute updates as incoming requests to the DC that you're working on. (For comprehensive documentation about replication, see the Microsoft TechNet article "How Active Directory Replication Topology Works" at bit.ly/hcbXJT.)

The Right Tools for the Job

Now that you have the basic concept under your belt, and you've presumably verified that all the underlying AD components are working correctly, what tools will you use to fix replication? The first thing to do is to run DCDIAG on the target DC to check its general health. DCDIAG is the main diagnostic utility for DCs. It runs a suite of 27 tests by default. For example, Figure 1 shows the Replications test failing for a DC named GODAN.

If a DCDIAG test results in warnings or failures, and if the reason for it isn't immediately obvious, you should rerun DCDIAG. In the follow-up run, focus on the specific test that failed, and specify verbose operation. In this case, DCDIAG /TEST:Replications /V provides little extra useful information; however, a follow-up run of the DCDIAG test on the source DC (Kyoshi) reveals that the directory service isn't running.

The next utility to concentrate on is REPADMIN. REPADMIN is the Swiss Army knife of replication utilities. It has 69 different commands in three tiers of increasing complexity, from simple checks to destroy-your-own-directory commands. As if that weren't enough, the syntax of commands often varies slightly between versions. Knowledge

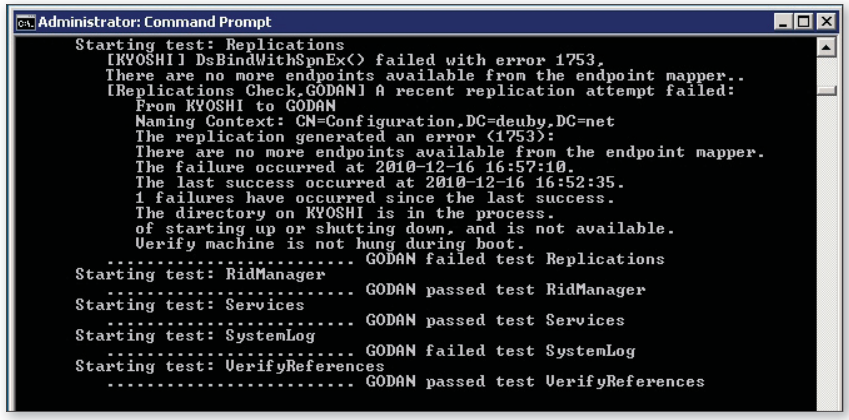


Figure 1: Results of running the DCDIAG tool Replications test for a DC named GODAN

of some of the more arcane REPADMIN commands is a requirement for directory service nerd-dom. You can use REPADMIN /?:*command* to get detailed help about individual commands in Server 2008 R2 or Server 2008. Table 1 shows a list of REPADMIN commands. (For information about how to use the Windows 2003 version of REPADMIN, see the Microsoft article "Troubleshooting replication with repadmin" at bit.ly/dJapAF.)

Generally, the first REPADMIN command to run is /SHOWREPL, which is targeted to the DC that's not receiving updates. Figure 2 shows the result. This is an intimidating result if you haven't looked at it before. The data is easier to understand if you break it into sections. The first section, preceding the dashed line, shows general information about the DC. In particular, the data shows that the DC is a Global Catalog server, and it shows the DSA GUID. The next section shows every partition, in distinguished name (DN) format, that this DC hosts. It also shows the DC's replication partner (and the partner's DSA GUID) and the time that the DC last replicated successfully.

Knowing Where to Look

Replication usually fails on a per-DC basis. So if you see replication from one partition failing and from another partition succeeding, this probably means that the partitions are replicated from different DCs. In this simpler case, restarting the KYOSHI NETLOGON service clears up the problem. After you obtain and study this detailed replication information, troubleshoot from the wire up to eliminate the most likely suspects. (For more help, you can refer to the replication page of my Active Directory Troubleshooting flowchart on my Active Directory Troubleshooting Tips and Tricks blog.)

If the replication problem that you're troubleshooting is between sites, first

Table 1: Common REPADMIN Commands

Command	Use	Common Options	Comments
/REPLSUMMARY	Replication summary of all DCs in the forest	/BYSRC /BYDEST /SORT:DELTA	Run daily
/SHOWREPL	Replication status of a single DC (or DSALIST selection)	/V, /REPSTO	First command for detailed replication troubleshooting
/SYNCALL	Trigger replication between a DC and its replication partners	DN of a single partition you want to sync	Easy command to force replication
/KCC	Trigger the Knowledge Consistency Checker to regenerate site topology		Use after you've changed site configuration and don't want to wait for the KCC to do it on schedule (15 minutes)
/REPLICATE	Trigger replication with a single partner	(Required) DSALIST and the DN of the partition you want to sync	Force replication with a single partner and partition
/QUEUE	See what changes are queued up for the target DC	None	Useful to see what changes are queuing up for a DC that has replication problems
/SHOWOBJMETA	Show attribute information (metadata) for a given object on a given DC	(Required) DSALIST and DN of the object	Run against the same object on two different DCs to determine whether an update to that object has replicated
/DSAGUID	Determine the Site\DC name from the DSAGUID	(Required) DC to run the command against (aka homeserver) and DSA GUID	Get the DC name from the GUID listed in many REPADMIN command outputs
/OPTIONS	Many different uses; see REPADMIN /?:OPTIONS	+/-IS_GC, +/-DISABLE_<INBOUND|OUTBOUND>_REPLICATION	Quick way to make a GC; basis of the "oops" command (tinyurl.com/264lcdd)
/BRIDGEHEADS	Discover the bridgehead servers for your site	DSALIST (required), /VERBOSE	"*" will list bridgehead servers for the forest
/ISTG	Discover the intersite topology generator for your site	DSALIST (required), /VERBOSE	"*" will list the ISTGs for the forest

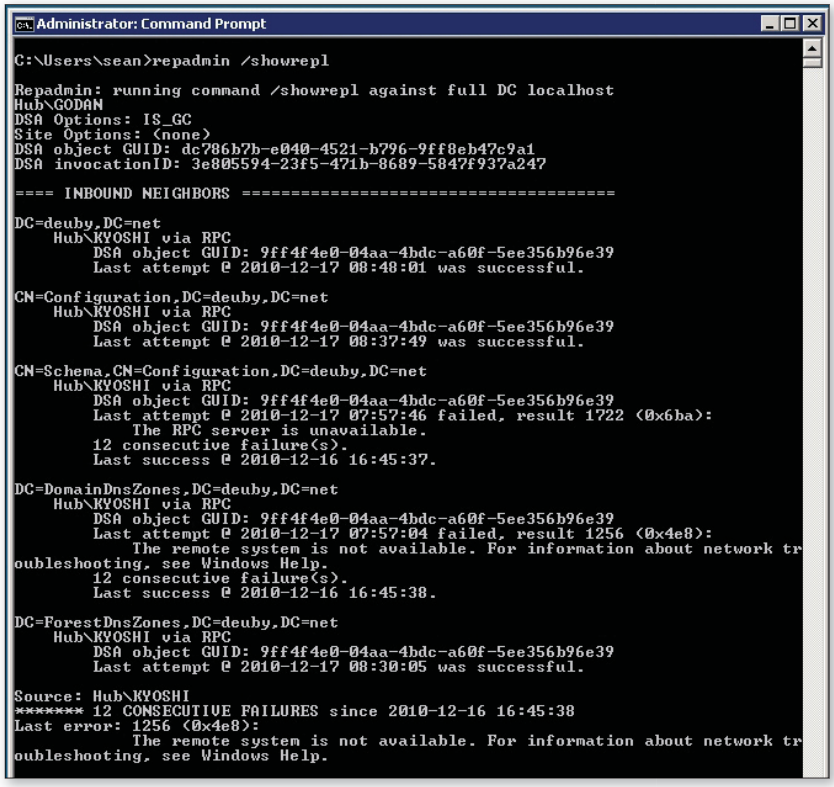


Figure 2: Results of running the REPADMIN command /SHOWREPL

check that the sites of the upstream and downstream DCs are connected to one other by site links. To learn which DCs are the bridgehead servers between these sites, run

```
REPADMIN /BRIDGEHEADS *
```

(The asterisk returns the bridgehead servers for all your sites.) Then, run

```
REPADMIN /FAILCACHE FSMO_ISTG:<site>
```

This command targets the intersite topology generator for the site that's represented by the *site* parameter. It also displays a list of failed replication links that are detected by its KCC. If the problem is caused by an incorrect site topology (e.g., someone moved a DC to a new site without creating a site link object to connect it to the other sites), or if you're simply moving DCs around, REPADMIN /KCC will force the KCC to recalculate and create connection objects between DCs so that you don't have to wait for its scheduled run.

When you think you've fixed the problem that's preventing replication, you can trigger general replication for all your target DC's partners by running

```
REPADMIN /SYNCALL
```

or for a specific partner and directory partition by running

```
REPADMIN /REPLICATE <targetDC>
  <sourceDC> <directory partition>
```

in which the directory partition is, for example, DC=Deuby,DC=net.

It's important to monitor replication on a regular basis so that you can correct any issues before they get out of hand. The easiest way to do this is to run

```
REPADMIN /REPLSUMMARY
```

regularly. Doing this provides you a replication summary of all the DCs in your forest. For deeper analysis, you can run

```
REPADMIN </command> *
```

(instead of using a DC name). This runs a REPADMIN command, such as /SHOWREPL, against every DC in your forest. Tim Springston, an escalation engineer in Microsoft's Premier Customer Support Group, has blogged about how to use REPADMIN's /CSV option to create an organized output of /SHOWREPL * that you can use to look at the replication status of all your DCs in Microsoft Excel. (See "Get the Lowdown on your Replication" at bit.ly/ek0Jic.)

Here's another tip that's no more technical than a dry erase marker: Use a large whiteboard when you troubleshoot replication issues between multiple DCs or sites. Otherwise, the complexity of the relationships between DCs, directory partitions, and sites will quickly make your head spin.

Finally, I want to put in a good word for an old replication tool that doesn't seem to get much respect: REPLMON. This utility is part of the Windows 2003 and Windows 2000 Support Tools, and it provides a graphical view of your replication topology. It can't do nearly as many things as REPADMIN, and some features don't work with Server 2008 R2 or Server 2008. But it's the best way to learn how DCs establish connections with one other. (I created a short screencast about REPLMON that will walk you through the basic steps. To watch it, visit youtu.be/GW2F0IzPblk. To obtain Windows Support Tools, visit the Windows Server 2003 Service Pack 2 32-bit Support Tools download page at bit.ly/dFUMzm.)

Bottom Line: Eternal Vigilance

AD replication is a process that's prone to failure. But most of the time, a supporting component is the cause of the problem. If you experience replication problems, check those AD foundations—physical, network, name resolution, the OS, and authentication—before you spend much time on AD itself or on the replication process.

If you correct the underlying problems and give AD a little time to reestablish its connections, many problems will simply disappear. Become familiar with REPADMIN and keep a good image of the underlying structure, and you'll keep your AD environment healthy.

InstantDoc ID 129333

Sean Deuby
(sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine*. He is a former technical lead of Intel's core Directory Services team, and has been a Directory Services MVP since 2004.

FEATURE

Creating Remote Sessions in PowerShell 2.0

How to connect to one or many remote computers

by Don Jones

When I first started using PowerShell, I was playing around with the Get-Service command and noticed that it had a -ComputerName parameter. Hmmm . . . does that mean it can get services from other computers, too? After a bit of experimenting, I discovered that's exactly what it did. I got very excited and started looking for -ComputerName parameters for other cmdlets. I was disappointed to find that there were very few.

What I've realized since then is that PowerShell's creators were a bit lazy—and that's a good thing. They didn't want to have to code a -ComputerName parameter for every cmdlet, so they created a shell-wide system called remoting. Basically, it enables any cmdlet to be run on a remote computer. You can even run cmdlets that exist on the remote computer but don't exist on your own computer, which means you don't always have to install every administrative cmdlet on your workstation. This remoting system is powerful and provides a number of interesting administrative capabilities.

PowerShell offers two distinct types of remoting: one-to-one (1:1) remoting and one-to-many (1:n) remoting. Before I tell you about them, though, you need to be familiar with the basics.

The Idea Behind PowerShell Remoting

PowerShell remoting works similar to Telnet and other age-old remote control technologies. When you run a command, it's actually running on the remote computer. All that comes back to your computer are the results of that command. Rather than using Telnet or Secure Shell (SSH), however, PowerShell uses a new communications protocol called Web Services for Management (WS-Management). The protocol operates entirely over HTTP or HTTP Secure (HTTPS), making it easy to route through firewalls if necessary because each protocol uses a single port to communicate. Microsoft's implementation of WS-Management comes in the form of a background service named Windows Remote Management. WinRM is installed along with PowerShell 2.0 and is started by default on server OSs like Windows Server 2008 R2. It's installed on Windows 7 by default, but the service is disabled. You only need to enable WinRM on those computers that you want to send commands to. The computer you're physically sitting in front of doesn't need WinRM running.

PowerShell cmdlets all produce objects as their output. When you run a command remotely, its output objects need to be put into a form that can be easily transmitted over a network using the HTTP or HTTPS protocol. So, PowerShell automatically serializes output objects into XML files. The XML files are transmitted across the network. When they reach your computer, they're deserialized back into objects that PowerShell can work with. Why should you care? Because those serialized objects are really just snapshots. They don't update themselves continually. That is, if you were to get the objects that represent the processes running on a remote computer, what you get back will only be accurate for the exact point in time at which those objects were generated. Values such as memory usage and

CPU utilization won't change. In addition, you can't tell the deserialized objects to do anything. For example, you can't instruct one to stop itself. That's a basic limitation of remoting, but it doesn't really stop you from doing some pretty amazing stuff.

There are just a few basic requirements to use remoting:

- Both your computer (aka local computer) and the one you want to send commands to (aka remote computer) must be running Windows PowerShell 2.0. Windows XP is the oldest version of Windows on which you can install PowerShell 2.0, so it's the oldest version that can participate in a remote session.
- Ideally, both the local and remote computers need to be members of the same domain or members of trusted/trusting domains. It's possible to get remoting to work outside of a domain, but it's tricky, so I won't be covering it here. To learn more about that scenario, see the PowerShell Help topic about_Remote_Troubleshooting.

WinRM Overview

Let's talk just a bit about WinRM because you're going to have to configure this service to start using remoting. Once again, you only need to configure WinRM and PowerShell remoting on the remote computers. In most of the environments I've worked in, the administrators have enabled remoting on every computer running XP or later. Doing so gives you the ability to remote into desktop and laptop computers in the background (meaning the user of those computers won't know you're doing so), which can be useful.

WinRM isn't unique to PowerShell. WinRM can route traffic to multiple administrative applications. WinRM essentially acts as a dispatcher. When traffic comes in, WinRM decides which application needs to deal with that traffic and tags that traffic with the name of the recipient application. Recipient applications must register with WinRM so that WinRM can listen for incoming traffic on their behalf. In other words, you not only need to enable WinRM but also register PowerShell as an endpoint with WinRM.

The easiest way to do both tasks is to open PowerShell as an administrator and run the Enable-PSRemoting cmdlet. You might see references to a different cmdlet named Set-WSManQuickConfig. There's no need to run that cmdlet. Enable-PSRemoting calls it for you and performs a few extra steps that are necessary to get remoting up and running. All told, the Enable-PSRemoting cmdlet starts the WinRM service, configures it to start automatically, registers PowerShell as an endpoint, and even sets up a Windows Firewall exception to permit incoming WinRM traffic.

If you're not excited about having to visit every computer to enable remoting, you can use a Group Policy Object (GPO) instead. The necessary GPO settings are built into Windows Server 2008 R2 domain controllers (DCs). Just open a GPO and navigate to Computer Configuration\Administrative Templates\Windows Components. Near the bottom of the list you'll find both *Remote Shell* and *Windows Remote Management (WRM)*, which you need to configure. The Help topic about_Remote_Troubleshooting provides detailed instructions on how to do so. Just look for the "How to Enable Remoting in an Enterprise" and "How to Enable Listeners by Using a Group Policy" sections within that Help topic.

WinRM 2.0 (which is what PowerShell uses) defaults to using TCP port 5985 for HTTP and 5986 for HTTPS. These ports help ensure WinRM won't conflict with any locally installed Web servers, which tend to listen to ports 80 and 443. You can configure WinRM to use alternate ports, but I don't recommend doing so. If you leave those ports alone, then all of PowerShell's remoting commands will run normally. If you change the ports, you'll have to always specify an alternate port when you run a remoting command, which means more typing for you. If you absolutely must change the port, you can do so with the command

```
Winrm set winrm/config/
  listener?Address=*
  +Transport=HTTP @{Port="1234"}
```

where *1234* is the port you want. (Although this command wraps here, you'd enter it all on one line. The same holds true for the other commands that wrap.) If you need to use HTTPS instead of HTTP, you can modify this command to set the new HTTPS port. I should admit that there is a way to configure WinRM on local computers to use alternate default ports, so that you don't have to constantly specify an alternate port when running remoting commands. But for now let's just stick with the defaults Microsoft came up with.

If you browse around in the GPO's Remote Shell settings, you'll notice that you can configure settings such as how long a remote session can sit idle before the server kills it, how many concurrent users can remote into a server at once, how much memory and how many processes each remote shell can utilize, and the maximum number of remote shells a given user can open at once. These settings help ensure that your servers don't get overly burdened by forgetful administrators. By default, however, you have to be an administrator to use remoting, so you don't need to worry about ordinary users clogging up your servers.

1:1 Remoting

With 1:1 remoting, you're basically accessing a shell prompt on a single remote computer. Any commands you run will run directly on that computer, and you'll see results in the shell window. This is vaguely similar to using Remote Desktop Connection, except that you're limited to PowerShell's command-line environment. PowerShell remoting uses a fraction of the resources that Remote Desktop requires, so it imposes much less overhead on your servers.

To establish a 1:1 connect with a remote computer named Server-R2, you'd run

```
Enter-PSSession -ComputerName Server-R2
```

Assuming that you enabled remoting on that computer, the computer is in the same domain, and your network is functioning correctly, you should get a connection going. PowerShell lets you know that you've succeeded by changing the shell prompt to

```
[server-r2] PS C:\>
```

The [server-r2] portion tells you that everything you're doing is taking place on Server-R2. You can then run whatever commands you like. You can even import any modules and add PowerShell snap-ins (PSSnapins) that happen to reside on that remote computer.

Even permissions are the same. Your copy of PowerShell will pass along whatever

security token it's running under. (PowerShell does this with Kerberos, so it doesn't pass your username or password across the network.) Any command you run on the remote computer will run under your credentials, so anything you have permission to do, you'll be able to do. It's really just like logging directly into that computer's console and using its copy of PowerShell directly. Well, almost. There are a couple of differences:

- If you have a PowerShell profile script on the remote computer, it won't run when you connect using remoting. Simply put, profiles are a batch of commands that automatically run each time you open the shell. People use them to automatically load shell extensions, modules, and so forth.
- You're restricted by the remote computer's Execution Policy. Let's say your computer's policy is set to RemoteSigned so that you can run local unsigned scripts. If the remote computer's policy is set to Restricted (the default setting), it won't be running any scripts for you when you're remoting into it.

Many PowerShell cmdlets come in pairs, with one cmdlet doing something and the other doing the opposite. In this case, Enter-PSSession connects you to the remote computer and Exit-PSSession closes that connection. The Exit-PSSession cmdlet doesn't need any parameters. After it runs, the remote connection closes and your shell prompt changes back to the normal prompt. What if you forget to run Exit-PSSession? Don't worry. PowerShell and WinRM are smart enough to figure out what you did and will close the remote connection.

I do have one caution to offer. When you're connecting to a remote computer, don't run Enter-PSSession from the remote computer unless you fully understand what you're doing. For example, let's say you work on Computer A. You connect to Server-R2. At the PowerShell prompt, you run

```
[server-r2] PS C:\> Enter-PSSession
  Server-DC4
```

Server-R2 is now maintaining an open connection to Server-DC4. This creates a "remoting chain" that's hard to keep track of. It also imposes unnecessary overhead on your servers. There might be times when you have to do this (e.g., Server-DC4 sits behind a firewall and you can't access it directly, so you need to use Server-R2 as a middleman). But, as a general rule, try to avoid remote chaining.

1:n Remoting

One of the coolest things in PowerShell is 1:n remoting. It lets you send a command to multiple remote computers at the same time—that's right, full-scale distributed computing. Each computer will independently execute the command and send the results back to you. It's all done with the Invoke-Command cmdlet in a command such as

```
Invoke-Command -ComputerName
  Server-R2,Server-DC4,Server12
  -Command { Get-EventLog Security
  -Newest 200 |
  Where { $_.EventID -eq 1212 } }
```

The command in the outermost braces gets transmitted to all three remote computers. By default, PowerShell talks with up to 32 computers at once. If you specify more than 32 computers, it will queue them up. Then, as one computer completes, the next one in line begins. If you have a really awesome network and powerful computers, you could raise that number by using the cmdlet's -ThrottleLimit parameter. You can read about how to use this parameter in the Invoke-Command cmdlet's Help page.

One item you won't see in that cmdlet's Help page is the -Command parameter, yet the command I just showed you works fine. The -Command parameter is actually an alias, or nickname, for the -ScriptBlock parameter that's listed in the Help page. I have an easier time remembering -Command, so I tend to use it instead of -ScriptBlock, but they both work the same way.

If you read the Help page for Invoke-Command carefully, you'll also notice a parameter that lets you specify a script file rather than a command. The -FilePath parameter lets you send an entire script to remote computers, which means you can automate some pretty complex tasks and have each computer do its own share of the work.

I want to circle back to the -ComputerName parameter for just a bit. In the sample Invoke-Command code, I used a comma-separated list of computer names. If you have a lot of computers, you might not want to type all their names every time you want to connect to them. Instead, you can create a text file that contains one computer name per line, with no commas, no quotes, or anything else. For example, if your text file is named webservers.txt, you'd use the code

```
Invoke-Command -Command { dir }
  -ComputerName (Get-Content
     webservers.txt)
```

The parentheses force PowerShell to execute the Get-Content cmdlet first—pretty much the same way parentheses work in math. The Get-Content cmdlet's results are then put into the -ComputerName parameter.

Querying computer names in Active Directory (AD) is also possible, but it's a bit trickier. You can use the Get-ADComputer cmdlet to retrieve the computers, but you can't stick that command in parentheses like you do with Get-Content. Why not? Get-Content produces simple strings of text, whereas Get-ADComputer produces computer objects. The -ComputerName parameter is expecting strings. If it were to receive computer objects, it wouldn't know what to do with them. So, if you want to use Get-ADComputer, you need to get the values from the computer objects' Name properties. Here's how:

```
Invoke-Command -Command { dir }
  -ComputerName (Get-ADComputer
  -Filter * -SearchBase
  "ou=Sales,dc=company,dc=pri" |
  Select-Object -Expand Name)
```

Within the parentheses, the computer objects are piped to the Select-Object cmdlet and its -Expand parameter is used to expand the Name property of those computer objects. The result of the parenthetical expression is a bunch of computer names, not computer objects—and computer names are exactly what the -ComputerName parameter wants.

In case you're unfamiliar with Get-ADComputer, let's take a look at what this cmdlet is doing. The -Filter parameter is specifying that all computers should be included in the output and the -SearchBase parameter is telling PowerShell to start

looking for computers in the Sales organizational unit (OU) of the company.pri domain. Get-ADComputer is available only on Windows Server 2008 R2 and on Windows 7 after installing the Remote Server Administration Tools. On those OSs, you have to run

```
Import-Module ActiveDirectory
```

to load the AD cmdlets into the shell so that they can be used.

But Wait, There's More

These examples have all been for ad-hoc remote sessions. If you're going to be reconnecting to the same computer (or computers) several times within a short period of time, you can create reusable, persistent sessions instead. That's especially helpful if the connection requires alternate credentials, a nondefault port number, or something else that requires additional parameters.

To create persistent sessions, you use the New-PSSession cmdlet, then save them in a variable for easy access. For example, the following code creates remote sessions with three computers, then stores them in the $sessions variable

```
$sessions = New-PSSession
  -ComputerName One,Two,Three
  -Port 5555
  -Credential DOMAIN\Administrator
```

The remote sessions close automatically when you close the shell, but until then they can take up memory and a tiny bit of CPU on both the local and remote machines. To explicitly close them, you can use the Remove-PSSession cmdlet

```
$sessions | Remove-PSSession
```

When you need to re-open the sessions, you can use the Invoke-Command cmdlet

```
Invoke-Command -Command { dir }
  -Session $sessions
```

or the Enter-PSSession cmdlet

```
Enter-PSSession
  -Session $session[1]
```

Note that in the Enter-PSSession code, only one remote session is being re-opened. The index number 1 tells PowerShell to re-open the session with the computer named Two. (It's a zero-based index.)

Extend Your Reach

PowerShell remoting has a lot of power and utility. If you use it, you'll find that it really extends your reach.

InstantDoc ID 129345

Don Jones
(powershell@concentratedtech.com) is the author of more than 35 books, and is a speaker at technology conferences such as Microsoft TechEd and Windows Connections. He's a multiple-year recipient of Microsoft's MVP and is technical guide for PowerShell at www.windowsitpro.com/go/DonJonesPowerShell.

FEATURE

Taking Advantage of iSCSI in Storage Server 2008 R2 Enterprise Edition

Learn how to set up and test Storage Server to harness the power of iSCSI

by John Howie

The iSCSI protocol is becoming increasingly popular in enterprise environments of all sizes. If you haven't heard of iSCSI, it's simply an adaption of the tried-and-true SCSI protocol used to connect servers to high-performance disk enclosures and CD-ROM drives. It uses TCP/IP over wired networks instead of dedicated cables. (Remember all those thick cables and huge plugs with delicate pin-outs?)

In recent months, iSCSI has become wildly popular in part because of the rise of virtualization, especially virtualization technology that allows running virtual machines (VMs) to be moved between different servers so that maintenance can be carried out on the host server without affecting the availability of the guest VMs. The only interconnectivity required between servers and the disks on storage subsystems is an IP network, which allows many servers to share the same storage subsystem. With older technologies, such as SCSI DAS, two servers at most could access a shared storage subsystem. Fibre Channel (FC)-based SANs can be built to permit multiple servers to access the same storage subsystem. But FC-based SANs are extremely expensive and require special HBAs to be installed on servers before the servers can connect to FC controllers, which are specialized switches that are fronting a SAN.

Using an IP network, iSCSI costs far less than the alternatives and offers more flexibility. You might already be using NAS in your environment. NAS uses common IP-based protocols, such as WWW Distributed Authoring and Versioning (WebDAV), NFS, Server Message Block (SMB), and Common Internet File System (CIFS), but these protocols are file-level protocols and are generally not up to the task of providing access to extremely large files, nor are they suited for high-performance solutions such as virtualization or databases. The block-level iSCSI protocol avoids performance and other problems associated with file-level protocols, including file locking.

A number of vendors offer a wide range of iSCSI solutions today, including NAS systems with iSCSI support. Microsoft recently released Windows Storage Server 2008 R2, which is an optimized version of Windows Server 2008 R2, with iSCSI support. Available in storage products from vendors like Dell, HP, and others, Storage Server boasts an impressive range of features that allow you to build storage subsystems. Those subsystems can be used to host the virtual disks of your VMs, host huge databases for your database servers, and do pretty much anything else you can think to throw at them. Storage Server also includes easy-to-use management features and deduplication software to minimize storage requirements. Best of all, Storage Server integrates seamlessly into your Windows network and also offers support for typical NAS protocols.

In this article, I'll describe how to set up and test Storage Server Enterprise Edition in your environment. Storage Server comes in Workgroup Edition, Standard Edition, and Enterprise Edition. An overview of the differences between the editions can be found at technet.microsoft.com/en-us/library/gg214172(WS.10).aspx. Although Storage Server is available only for use in production

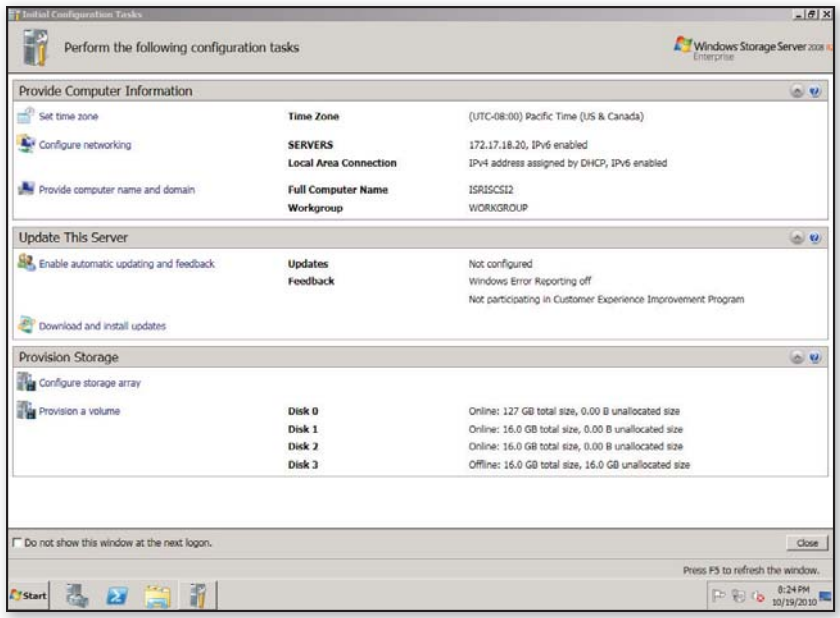


Figure 1: The Initial Configuration Tasks screen

environments in products from OEMs, if you have a TechNet subscription, you can download Storage Server as an update to Server 2008 R2. You can then test it in a physical or virtual environment. For more details about downloading and using Storage Server, see blogs.technet.com/b/josebda/archive/2010/09/27/windows-storage-server-2008-r2-and-the-microsoft-iscsi-software-target-3-3-are-available-on-msdn-technet-here-s-how-to-install-them.aspx.

Preparing for and Performing Initial Setup

Before deploying Storage Server, you need to prepare your environment. You should allocate a static IPv4 address for Storage Server, and if you use IPv6, allocate an IPv6 address. The IPv4 and/or IPv6 address will be used to remotely connect to Storage Server to manage it, and for the Storage Server to communicate with domain controllers (DCs), DNS servers, and other equipment. You don't need to join a Storage Server system to a domain, but I recommend doing so for ease of management. It's possible to run both iSCSI and other network traffic over the same network using a single NIC on your member servers and the Storage Server machine in low-volume scenarios, but I wouldn't recommend this configuration in a production environment. Typically, you'll dedicate a NIC on each member server just for communicating with Storage Server on a network dedicated to iSCSI traffic. When using dedicated NICs, allocate IPv4 and IPv6 addresses for Storage Server that will be used by iSCSI clients, which are also known as iSCSI Software Initiators. You can use RFC 1918 non-public IPv4 addresses in the following ranges for your iSCSI network: 10.x.x.x, 172.16.x.x – 172.31.x.x, and 192.168.x.x. Later, I'll discuss additional security considerations.

When you first start Storage Server and log on using the default username and password from the OEM that built your server, you'll be presented with an Initial Configuration Tasks (ICT) screen customized for Storage Server and similar to that shown in Figure 1. Each OEM can configure the ICT screen—for example, to add tasks for creating and managing two-node Storage Server clusters for fault tolerance and resiliency. Your first steps should be to configure the time zone, IP addresses, and host name, and to domain-join Storage Server. Next, download and install updates. I recommend that you not enable automatic updating for production environments because you don't want your Storage Server system to reboot in an uncontrolled fashion after installing updates, making the shares and volumes it serves unavailable.

Provisioning and Serving NAS Using SMB and NFS

From the ICT screen, you can click the option *Provision a volume,* which launches the Provision Storage Wizard. You'll have the option to provision storage on one or more disks that are attached to the server, that are online and initialized, and that have unallocated space. If your disks are offline or haven't yet been initialized, you'll have to use Disk Management under the Storage node in Server Manager to bring the disks online and to initialize them before the wizard will recognize them. You'll also have the opportunity to provision storage on storage subsystems, such as SANs, if Storage Server fronts a storage subsystem. Stepping through the wizard allows you to select the unallocated storage, choose the amount you want to allocate, decide where to mount the storage when allocated, and select the options to use when formatting the storage. When you create storage, you can choose to launch the Provision a Shared Folder Wizard, which takes you through the steps of creating a new folder, setting permissions to it, and sharing it using SMB and (if you have Server for NFS installed on Storage Server) NFS.

Figure 2 shows the new Microsoft Management Console (MMC) Share and Storage Management snap-in in Storage Server,

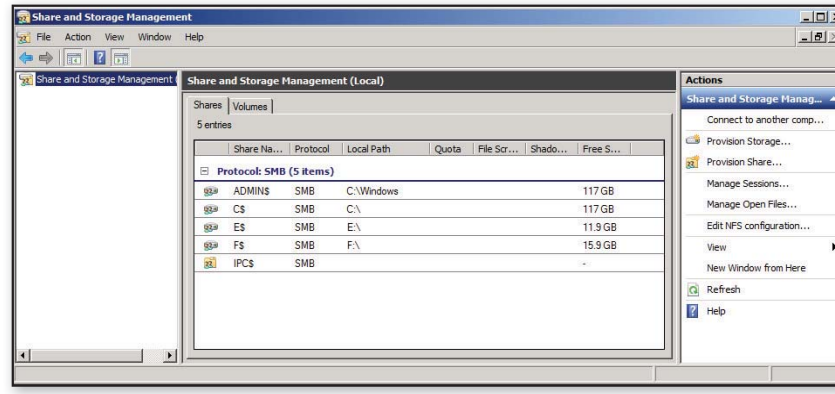


Figure 2: The Share and Storage Management snap-in

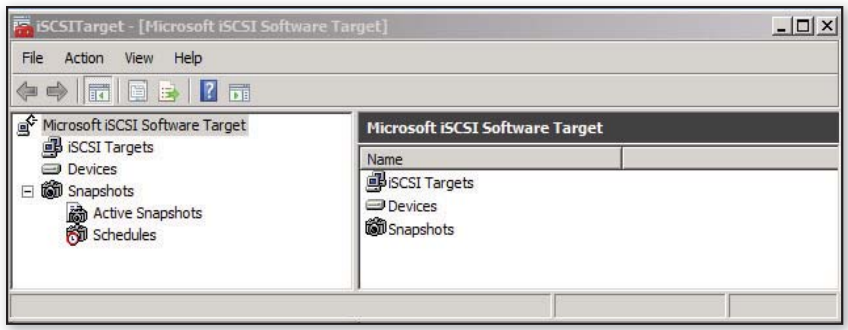


Figure 3: The Microsoft iSCSI Software Target MMC snap-in

available from the Administrative Tools folder on the Start menu. From the snap-in, you can launch the Provision Storage Wizard and the Provision Share Wizard. You can also manage open sessions and files and configure NFS if it's enabled. You don't need to use the Provision Storage Wizard nor the Provision a Shared Folder Wizard to manage disks, volumes, and shares. You can perform all these tasks from Disk Management in Server Manager and from Windows Explorer. You can also use the command line and Windows PowerShell as you would on Server 2008 R2. The MMC snap-in and wizards make the tasks easier to accomplish for inexperienced administrators.

Storage Server and iSCSI

Storage Server Enterprise Edition includes iSCSI target software. With this software, you can serve iSCSI clients using the iSCSI protocol. Managing iSCSI on Storage Server isn't as easy as provisioning and serving NAS using SMB and NFS. Before you start working with iSCSI in Storage Server, you'll need to understand how it works. When Storage Server is used as a NAS server, you share folders, but when you use iSCSI, Storage Server serves whole drives to clients. The drives themselves aren't physical drives on Storage Server. Rather, they're virtual disks implemented as Virtual Hard Disk (VHD) files stored on volumes across one or more physical drives. This separation of iSCSI virtual disks, volumes, and physical drives isn't unique to Storage Server and can be found in other iSCSI server implementations.

This separation does come with many advantages. You can create iSCSI virtual disks that are the right size for the clients that will use them, freeing you from creating iSCSI disks that are the same size as physical drives. A physical drive can hold one or more volumes each with one or more VHDs. Alternatively, a volume can span multiple physical drives and hold one or more VHDs. Another advantage is that you can move the VHDs representing the virtual disks served by Storage Server to different volumes or even to different servers as needed.

Virtual Disk Management

You create a VHD file in Storage Server using the MMC Microsoft iSCSI Software Target snap-in, which Figure 3 shows. You can find this snap-in in the Administrative Tools folder on the Start menu. Right-click the Devices node, and select Create Virtual Disk from the context-sensitive menu to launch the Create Virtual Disk Wizard. As you step through the wizard, you'll be asked for the location and name of the VHD file representing the virtual disk, the size of the virtual disk in megabytes, and a description of the virtual disk. You'll also be prompted to specify the iSCSI targets that can access the virtual disk. You can specify the iSCSI targets later.

On Storage Server, you can mount the virtual disks, and initialize, format, and assign a drive letter to them through Windows Server's standard Disk Management snap-in. This allows you to prepare the virtual disks before serving them to iSCSI clients. Mounted disks can also be backed up using your standard backup software. To mount a disk, select the virtual disk in the Microsoft iSCSI Software Target snap-in, right-click it, select Disk Access, and click Mount Read/Write. You can dismount a virtual disk by right-clicking the disk, selecting Disk Access, and clicking Dismount.

You can create snapshots of virtual disks using the Microsoft iSCSI Software Target snap-in by right-clicking a virtual disk and selecting Create Snapshot. Snapshots can be mounted just like virtual disks. You can also roll back a virtual disk to a snapshot and export it. When you export a snapshot, you make it available to iSCSI clients just like a regular virtual disk. You can delete snapshots when they're no longer required.

It's possible to configure Storage Server to take regular snapshots using the Schedule Snapshot Wizard, which you can launch by right-clicking the Schedules node under the Snapshots node. A schedule can perform one of two actions: snapshot virtual disks, or snapshot virtual disks and mount the snapshots locally on the server. A snapshot schedule can snapshot all virtual disks or just the virtual disks you select, and snapshots can be taken on a daily, weekly, monthly, or one-time-only basis. Within each period, you can select the day and time of the snapshot.

Serving Virtual Disks to iSCSI Clients

Once you've created virtual disks, you need to specify iSCSI targets, which are used by iSCSI clients to mount the disks locally.

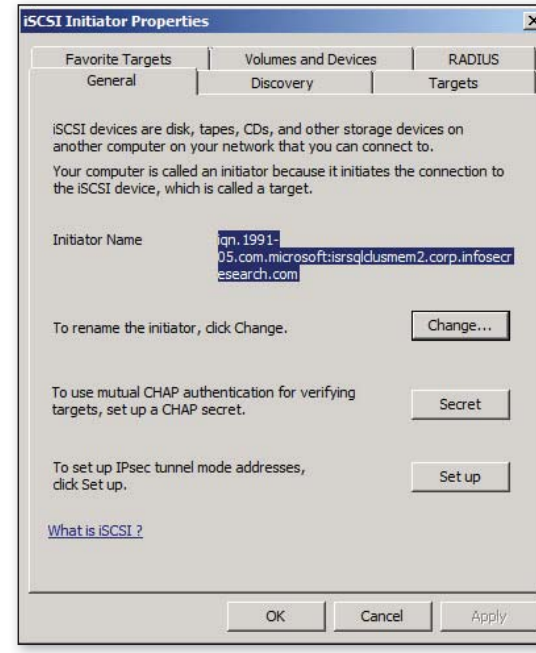


Figure 4: The iSCSI Initiator Properties General tab

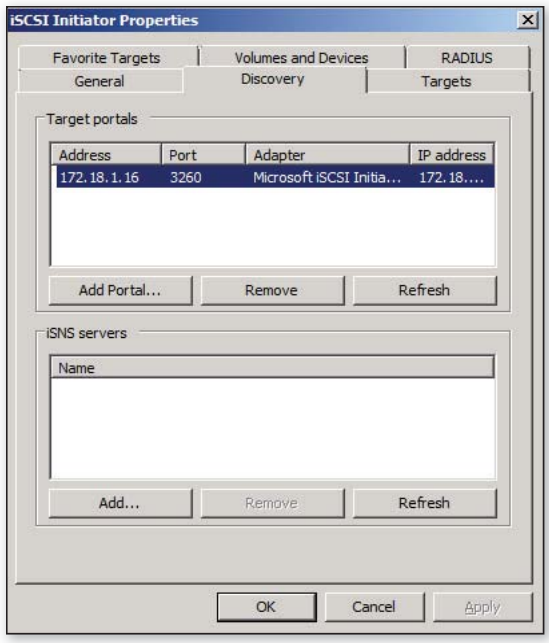


Figure 5: The iSCSI Initiator Properties Discovery tab

An iSCSI target is associated with a virtual disk. To create an iSCSI target, right-click the iSCSI Targets node, and select Create iSCSI Target to launch the Create iSCSI Target Wizard. After the introduction page in the wizard, the first step asks you to specify a name for the iSCSI target and an optional description. The target name is used by iSCSI clients to specify and connect to the target. The iSCSI target name can contain only letters and numbers without spaces.

The second step asks you to enter the iSCSI Qualified Name (IQN) of the iSCSI initiator (the iSCSI client) that will connect to the target. On Windows Server–based iSCSI clients, you can find the IQN by running the iSCSI Initiator program from the Administrative Tools folder on the Start menu. Figure 4 shows you where to find the IQN. You can list multiple IQNs for a target. You can also specify iSCSI clients by Fully Qualified Domain Name (FQDN) and by IP address instead. Once a target is created, associate a virtual disk by right-clicking it and selecting either the option to create a virtual disk or the option to add an existing virtual disk. You can add multiple disks to a target if you wish. Each virtual disk you add to a target is given a unique Logical Unit Number (LUN), just like a regular SCSI subsystem. The iSCSI client references each virtual disk using its LUN.

To access an iSCSI target, an iSCSI client is configured using its iSCSI initiator. To add a target, it must first be discovered by clicking the Discovery tab, clicking the Add Portal button, and specifying the IP address of Storage Server. The IP address is the IP address of the dedicated iSCSI network NIC, as Figure 5 shows. Once a target is discovered, it's listed on the Targets tab and will be listed as Inactive. Selecting an inactive target and clicking the Log On button allows you to connect to the target. You can specify that the connection to the target should be restored every time the computer starts.

On both the iSCSI target and the initiator, you can specify additional configuration options, such as the source IP address, which is typically the IP address of a NIC on a dedicated iSCSI IP network. Unless you run into difficulty connecting an initiator to a connector, I recommend you simply accept the default options.

When the iSCSI initiator logs on to a target, the disks are made available and visible in the Disk Management snap-in. The disks will be offline by default and must be brought online. Unless you mounted the disks on Storage Server and prepared them, you'll need to initialize and format the disks on the iSCSI client before you can assign them to a drive letter or mount them onto an empty folder on an NTFS volume.

iSCSI Security

In production environments, you probably go to great lengths to physically secure your hosts and data. When you use iSCSI, you introduce potential risks. If malicious insiders or (even worse) hackers outside your network could gain access to the iSCSI network, they would potentially be able to eavesdrop on iSCSI traffic and obtain sensitive data. They might also be able to connect to an iSCSI target and mount an iSCSI virtual disk onto their machine and access it, bypassing any file system controls, such as DACLs, if they know how.

Fortunately, there are several steps you can take to minimize the risks. First, as I described earlier, you should create a dedicated iSCSI network, and you should ensure that no traffic can be routed to or from this network. All routers, switches, and other equipment should be dedicated to the iSCSI network. Second, it's possible to use the Challenge Handshake Authentication Protocol (CHAP), which uses a shared secret known to the targets and the initiators to restrict access. You can also use mutual CHAP, in which a pair of secrets must be known to the initiator and the target. For authentication, it's also possible to use RADIUS, which is stronger than CHAP alone.

Although it's possible to restrict access to a target to only those initiators who know the shared secret, CHAP won't prevent an eavesdropper from gathering sensitive data by simply monitoring communications between initiators and targets. The Microsoft implementation of iSCSI Initiator and Target supports IPsec using a shared secret, which can be employed to encrypt traffic between initiators and targets. Note that there is a performance overhead when using IPsec, which might make it less appealing for demanding environments.

Tip of the Iceberg

I've only touched the surface of the features that Storage Server provides. Storage Server is an enterprise-ready, NAS, and iSCSI solution that integrates seamlessly into your Windows networks. Its deduplication technology helps you save disk space, and it can be deployed in fault-tolerant configurations to provide high-reliability solutions. Although it might seem daunting at first, once you've installed Storage Server and started using iSCSI, you'll find it to be amazingly flexible and almost second nature to use.

InstantDoc ID 129372

John Howie
(jhowie@microsoft.com) is a senior director at Microsoft where he manages several teams responsible for day-to-day security of the Microsoft cloud infrastructure. John is a visiting professor at Edinburgh Napier University and is co-chair of the Subject Matter Expert Working Group for Cloud Security Alliance.

FEATURE

SharePoint Governance Using COBIT 4.1

A framework to minimize risks and create predictable outcomes

by Dave Chennault

Governance for SharePoint isn't a checklist of administrative settings or server architectures. It's a set of policies and procedures that work together to minimize risks and create predictable outcomes at every stage of your SharePoint deployment. I'd like to show you a new framework for SharePoint governance from the recently published book, *SharePoint Deployment and Governance using COBIT 4.1: A Practical Approach* (ISACA). The first three chapters and a section on SharePoint in the cloud can also be found on Microsoft TechNet at technet.microsoft.com/en-us/library/ff758651.aspx. An online tool to track progress and the information associated with the governance framework is scheduled for release in spring 2011.

Let's look at an ungoverned SharePoint deployment and the unexpected effects that can follow. Then I'll review the Control Objectives for Information and Related Technology (COBIT) governance framework and provide a set of actions you can take to start governing your SharePoint deployment. Finally, I'll discuss governing SharePoint in the cloud.

Results of Improper Governance Practices

Deploying SharePoint can spawn unexpected results when you don't prepare the organization with proper governance practices. In 2008, I was leading a SharePoint consulting group for a large, national system integrator. A billion-dollar clothing manufacturer asked us to create a plan to use SharePoint 2007 to automate the creation and approval of refund checks that were created after distributors returned unsold merchandise to the company.

When we were called in, we found a check request and approval system that was a manual process using email to move Microsoft Word and Excel files among different approvers and the accounting team. This important business process resulted in millions of dollars of refund checks per quarter. Each refund request typically required five to eight weeks to process—this last point is very important to our case study.

My team was the integrator for this effort, which represented the manufacturing firm's first deployment of SharePoint. The system was developed and rolled out in 12 weeks, and the time to process refund checks was cut from several weeks to a few days. The new SharePoint solution streamlined processes even more than first anticipated.

Several weeks later, my phone rang. It was the CFO. "Your system just made me miss my number for the quarter! We cut too many refund checks too quickly and your system negatively impacted our cash position. Fix it, or I will rip out the whole system and go back to manual processing."

We hadn't expected that result. We had optimized the process too much. Now we needed to get the system governed to match business requirements, so we put in place technical and process fixes to slow refund processing down and regulate how quickly refund checks were issued.

Guiding Principles

You need to look at the system holistically within the context of the organization and the relationships between all components and systems affected by SharePoint. Governance of SharePoint has to be led by business and enabled by IT. I've seen organizations trying to understand SharePoint after it has been deployed without any idea of what problem it was supposed to have solved. Setting up SharePoint and saying to the business, "Come on in," results in a jumble of disjointed, one-off sites, ghost towns with stale content and no visitors. This approach increases exposure to risk because nearly everything is indexed and searchable. Also, IT is often ill-prepared for the wave of support and enhancement requests and the usage spike that we and others have called the "SharePoint Effect." Clearly, a framework that takes all of these factors into consideration is needed. That framework is governance.

My real-world experience leads me to conclude that SharePoint governance should be based upon the following principles:

- Business needs should lead technical decisions, not the other way around.
- SharePoint requires controls and repeatable processes to ensure its orderly deployment, operation, and maintenance.
- A team of senior business and technical users is required to set policies and procedures and to guide the ongoing deployment of SharePoint.
- Management reviews should be built into governance policies and procedures.
- IT resources, including staff and systems, should be leveraged and integrated into SharePoint.
- The framework should be built upon internationally recognized governance standards.
- The framework should be applicable at any stage of deployment or maintenance.

Such a framework is COBIT, created by the Information Systems Audit and Control Association (ISACA). Let's look at COBIT and how it has been applied to govern SharePoint.

COBIT

COBIT offers a comprehensive checklist of procedures and objectives to think about at every stage of SharePoint deployment. Now in its fourth version, it enables IT and business owners to work toward common goals while identifying and controlling risks. It builds on four domains to govern IT systems: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Divided among the four domains are 34 processes, high-level directives that form the goals for each domain. For example, the Plan and Organize domain includes the following 10 processes:

- P01 Define a Strategic Plan
- P02 Define the Information Architecture
- P03 Determine Technological Direction
- P04 Define the IT Processes, Organization, and Relationships
- P05 Manage the IT Investment
- P06 Communicate Management Aims and Direction
- P07 Manage IT Human Resources
- P08 Manage Quality
- P09 Assess and Manage IT Risks
- P10 Manage Projects

Each process has a set of suggested activities called control objectives that either mitigate risk or contain specific guidance or activities designed to help meet each facet of that process. For example, process P02, *Define the Information Architecture*, has the following four control objectives:

- P02.1 Enterprise information architecture model
- P02.2 Enterprise data dictionary and data syntax rules
- P02.3 Data classification scheme
- P02.4 Integrity management

Applying COBIT in the Real World

After attempting to apply COBIT "out-of-the-box" to a few SharePoint deployments, I decided that its processes needed to be rearranged outside of their domains and placed within phases that more closely mirrored the lifecycle of a SharePoint deployment. In *SharePoint Deployment and Governance using COBIT 4.1: A Practical Approach*, all 34 COBIT processes are spread across phases of an iterative software development lifecycle as Figure 1 shows. We tailored control objectives to meet the specific needs of a SharePoint deployment for each of the 34 processes. Consider the four control objectives that are defined for the DS1 *Define and Manage Service Levels* process (which you can also see in the Plan for Launch phase in Table 1 in this article at www.sharepointpro connections.com):

A. Develop or review service level framework

B. Define services and service level agreements for SharePoint

C. Define searching requirements, including scope and result set

D. Define index requirements and schedule

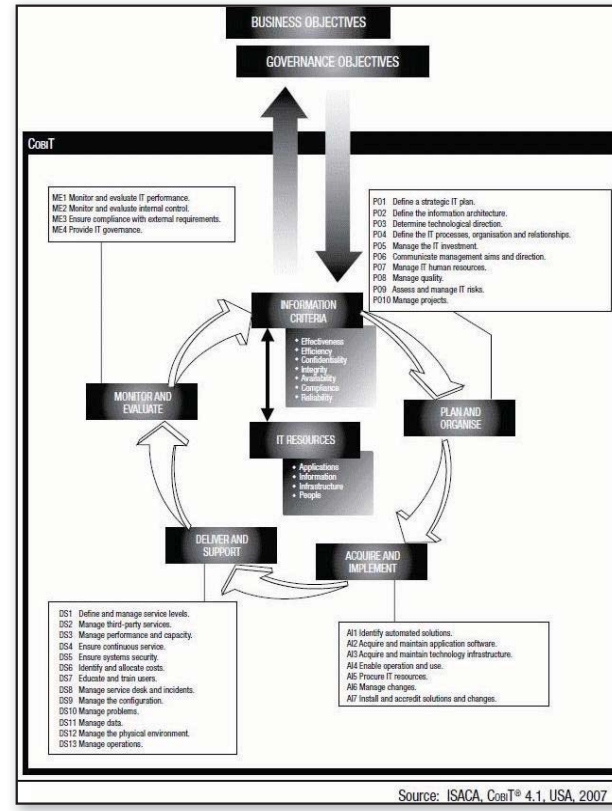


Figure 1: COBIT framework with processes mapped to domains

		Phase		Nintex Workflow	Nintex Reporting	SCOM	ScriptLogic ACL Auditing	SPBPA	Msf
Scope									
		P01 - Define a Strategic Plan							
8	A	Create a Steering Committee							
6	B	Identify Strategic Goals							
5	C	Identify Participating Business Units							
2	D	Map Business needs versus SharePoint Functionality							
8	E	Identify Key Business Owners for each Initiative							
-	F	Set Priorities							
		P02 - Define Information Architecture							
2	A	Identify Scope of Site Types in Deployment							
3	B	Identify Site Owners							
-	C	Identify Roles							
-	D	Develop a process for site request, approval, creation and auditing							
Plan for Launch									
		P03 - Determine Technological Direction							
1	A	Align business requirements with SharePoint Capabilities							
6	B	Evaluate Email Integration Options with SharePoint							
1	C	Identify integration opportunities with existing systems							
2	D	Identify MS Office integration needs							
1	E	Identify integration opportunities with existing content stores							
		P04 - Define Processes, Organization, Relationship							
2	A	Identify Tactical Team Members and Responsibilities							
5			Identify Operations Team and Responsibility						
3			Identify Support Team and Responsibility						
3			Identify Development Team and Responsibility						

Figure 2: Tool and maturity matrix for all controls

As you drill into each of the control objectives, specific actionable items are listed in a prescriptive fashion to guide your governance effort. These control objectives are a starting point rather than a comprehensive list. There can be many more items that are specific to your environment.

A matrix pulls it all together, listing the maturity of all control objectives within each deployment phase and procedure. (Figure 2 shows a portion of the matrix.) The cells that are darkened indicate the tool listed at the top of the column can be used to meet the control objective. Each of the darkened cells has a maturity model behind it (as Figure 3 shows), creating a scorecard with a calculated value of meeting the objective to the organization.

Implementation: Getting Started

The framework and all the procedures and control objectives are explained in the book, so don't worry if this article seems a bit much at your first reading. Let's look at how to use the framework to start governing SharePoint.

Step 1: Meet with IT and PM Staff

The governance process begins with a meeting of key IT resources participating in the SharePoint initiative. This meeting should be conducted in a workshop setting that can span multiple sessions. Here's a general guide to what should be accomplished with IT staff in this meeting, prior to meeting with key business stakeholders:

1. A SharePoint governance champion should be identified to guide the initial governance activities outlined within this section. Often this is a member of the IT staff or an outside consultant. The governance champion is responsible for all of the activities leading up to a self-sustaining SharePoint governance framework and steering committee.

The governance process begins with a meeting of key IT resources participating in the SharePoint initiative.

2. The governance champion should begin the governance initiative by identifying the relevant staff associated with SharePoint and their roles. These individuals will likely be later assigned to infrastructure, support, and development teams, or to the steering committee.

3. If SharePoint has been deployed, a survey should be created of current SharePoint sites, including a site map. Also, any documentation associated with the current deployment should be reviewed. This is similar to COBIT 4.1 process PO2, *Define the Information Architecture*.

4. Significant risks to adopting governance for SharePoint should be identified, which might include

- Inadequate executive sponsorship and direction
- Unwillingness of IT to support business needs
- Inability of the governing body to make decisions
- Internal staff or third parties not following the policies and procedures set by the governing body
- IT staff not following policies and procedures
- SharePoint being deployed widely across the organization, and current users being resistant to governance
- The business demanding service levels not possible within the allocated budget or technology
- The business demanding system features and functionality not possible within the allocated budget or technology

5. If SharePoint is currently deployed, the content stored there should be

Control Scorecard			
Process - AI5 - Procure IT Resources		Completed By	Dave Chennault
ID: AI5 -1	Name: Review HR Recruiting/Contracting process including: 1 - Sourcing agreements 2- Confidentiality Agreements, 3 - Screening procedure	Date	3/3/2010
Description			
within this control include a review of sourcing agreements with outside vendors. Questions such as how were the sourcing partners selected, are they in the best interest of the organization, do they meet legal and ethical requirements. A review of confidentiality agreements and how they are administered and tracked should also be conducted with particular attention to ensuring 100% compliance. Finally, periodical reviews should be held to determine how candidates are screened and if the best candidates are being gleaned from the pool of applicants.			
Progress Maturity (0-10)	Discussion - Progress To Date		
8	The organization is making great strides toward meeting the control objectives associated with the process. Sourcing agreements have been reviewed and appear to be both legally appropriate and in the best interest of the organization. All applicants are required to complete a non disclosure agreement and an initial review of the screening process of applicants has been completed		
	Non-compliant Areas Requiring Improvement		
	Areas that require additional improvement include developing a system to track all NDA forms, conducting periodical reviews of competitive technical sourcing capabilities and rates and periodical reviews of how applicants felt the application process worked.		
Benefits of Compliance	Discussion / Likelihood	Cost and Difficulty to Implement/ Description of Ben	Annual Benefit
- Higher Quality Staff	Regular reviews of how HR sourcing agreements and how partners are selected will lead to a better pool of applicants for open positions. It is very likely this will improve the quality of staff at the organization and improve the productivity of the staff by at least 10% / Likelihood 30%	4 hours by one resource to review existing process and recommend improvements/ Expect a 10% improvement in productivity as a result of saving 2000 hours of labor at $32.50 cost per hour	$ 65,000.00
- Lower Costs to Organization	Regular reviews of agreements will lead to lower costs since the existing agreements will be benchmarked against current practices / Likelihood 70%	4 hours per quarter/ Expect 10% savings in contract co	$ 15,000.00
- Protection of Trade Secrets via the NDA	Assuring 100% compliance with executing NDA agreements with all applicants and staff will ensure that proper steps are being taken to protect valuable intellectual property of the organization. / Likelihood 80%	40 hours to review existing NDA's and develop tracking system/ Expect at least 200 hours of savings in legal fees at $125/hr cost	$ 25,000.00
Risks of non-compliance	Discussion & Likelihood	Description of cost of non-compliance	Annual Cost Avoidance
- Low Quality staff	Lower quality of staff will result in additional training, lower quality output, higher re-work and additional staffing costs. / Likelihood 90%	2 weeks of training at $7500 per week, 10% less productivity at 2000 hours of labor at $32.50 cost and 200 hours of rework at $32.50 per hour	$86,500
- High cost of staff recruiting	"Sweetheart deals" and doing business because it has always been done that way results in higher costs to the organization for staff Likelihood 60%	Estimate 5% in additional cost by doing business via "sweetheart" deals and non competitive bidding. $90,000 spent on recruiting per year so saving s equal $4500.	$4,500
- Sourcing vendor could reveal staffing requirements to competitors revealing plans and strategic direction.	Sourcing vendor could reveal requisitions revealing strategic plans and needs / Likelihood 25%	indeterminate	$0
- Additional legal and administrative fees	Lack of an organized system to ensure NDA compliance and tracking will result in additional administrative fees to locate and manage NDA form and increased legal fees to protect the organization. Likelihood 80%	Estimate and additional 200 administrative hours of tracking NDA forms at $12.50/hour and an additional 80 hours saved in legal and civil litigation at $125 per hour.	$27,500
Mitigation Controls	Discussion & Likelihood		Cost
NDA's should be executed with all sourcing vendors	All vendors should execute NDA and these should be tracked by the legal department. - Estimate 2 man days at $500/day to develop. - Likelihood 95%		$1,000

Figure 3: Control scorecard with maturity model

reviewed and listed in detail, including content users and document retention schedules.

6. Create a list of requested business initiatives considered "in scope" by the IT department for the SharePoint deployment. If SharePoint is already deployed, list initiatives that are desired and include key stakeholders associated with each initiative.

7. Conduct an operational review. A representative sample includes the following:

- Backup requirements—Conduct a review of backup and recovery requirements and practices for any existing or planned SharePoint initiatives. This activity begins building information required to meet control process DS4, *Ensure Continuous Service*.
- Backup practices—If SharePoint has been deployed, conduct a review of backup practices for existing SharePoint deployments. This activity also builds information required to meet DS4.1.
- Review of cost allocation—This activity icludes how costs for SharePoint are or will be allocated to system users.
- Review of how change requests are managed—This activity includes how requests are logged and evaluated.
- Review of security—This activity includes reviewing how security requirements are implemented.
- Review of training—This activity encompasses a review of training plans and training materials in place.
- Review of Help desk processes—This activity includes a review of Help desk capabilities currently in place.

After the workshop, the following activities should be completed with IT leadership. These should be done prior to a final follow-up meeting with the entire IT team:

Findings and risk assessment review. The collected data should be summarized into a written report that identifies the maturity of the current SharePoint governance process and outlines the risks facing the organization. This report should

be reviewed with the IT team to validate findings and agree upon readiness and the desired next steps to implement SharePoint governance.

Decision to proceed with governance initiative. A frank discussion should be held with the IT leadership team to assess the organization's readiness to proceed with implementing governance for SharePoint. Any key impediments identified in the workshop should be evaluated and mitigated or compensated for prior to embarking upon the governance initiative. If the impediments are deemed significant enough to stop the governance framework, a plan should be devised to overcome each item prior to beginning.

Preliminary scorecard. If the decision to proceed with the governance initiative is approved, a preliminary survey should be conducted to assess the current state of governance using the maturity model control scorecard, which Figure 3 shows. The scorecard should track governance progress and highlight areas requiring additional attention.

Plan. A scope and timeline indicating which portions of the COBIT 4.1 framework will be adopted, including approach and timing, should be developed. This plan should be shared with the business units participating in the governance initiative to get their buy-in and input.

Tools. A review of required tools should be compiled.

Budget and plan. A preliminary budget and plan should be developed so that funds and resources required for the effort can be allocated.

After these activities have been completed, and if there are no significant impediments remaining, the organization is ready to begin the governance process in earnest.

Step 2: Meet with Business Stakeholders

After the initial meeting with IT staff outlined in the first step, key business stakeholders should be invited to a workshop to review findings and create the management team for the SharePoint governance initiative. Items to review should include key findings, such as business impact, and associated risks and costs of the current or proposed SharePoint deployment and plan. The activities involved include the following:

Hold a workshop. Key business stakeholders and IT staff should be invited to review the findings outlined in the first step. Candidates selected as key business stakeholders should be reviewed and added to a pool of prospects for the SharePoint governance steering committee. This begins to build the list of candidates required to satisfy one of the objectives of process PO1 *Define a Strategic IT Plan*.

Create a steering committee. After the candidates for the steering committee have been identified, the SharePoint governance champion should review the candidates and form a list. These candidates should be given the opportunity to accept or decline an invitation to join the steering committee, and a meeting should be set.

Hold the initial steering committee meetings. After the team has been identified, initial meetings should be held to lead the governance initiative. Sample agendas for the first three meetings are in *SharePoint Deployment and Governance using COBIT 4.1: A Practical Approach*.

Step 3: Move Ahead

After a functioning steering committee is in place, attention can be focused on satisfying the requirements of the processes and controls needed to govern SharePoint properly. The steering committee should review the governance initiative and reaffirm its commitment to these goals.

SharePoint Governance in the Cloud

Governance is just as important for cloud-based and hosted SharePoint as it is for on-premises deployments. You need to consider the following:

- The system will be operated by and cared for by staff you will likely never meet.
- The provider will probably require concessions on your part if you are working in a multi-tenant environment. Specifically, it will limit what you can and can't run. Care should be given to throttling considerations and the use of any server-side code that's outside of the sandbox in SharePoint 2010, as it will likely not be allowed.
- Backup processes and service level agreements (SLAs) are generally standardized and not subject to a lot of negotiation without a substantial fee increase.
- Pay attention to monitoring capabilities. Cloud and hosted solutions usually have strict SLAs that should be monitored closely as part of your governance planning. Provisions to access the data center and system statistics and logs should be included in your contracts.

All of these considerations will have substantial impacts on the functionality and technological direction of the system and should be considered in your governance planning.

> A strong governance framework and adherence to it will help you realize maximum benefit for your SharePoint deployment while minimizing risk to the organization.

Maximum Benefit, Minimum Risk

A strong governance framework and adherence to it will help you realize maximum benefit for your SharePoint deployment while minimizing risk to the organization. COBIT 4.1 from ISACA offers the best governance framework currently available. Molding it to fit your SharePoint needs will help you successfully deploy and manage SharePoint whether on-premises or in the cloud.

InstantDoc ID 128968

Dave Chennault (DaveC@skylitesystems.com) is president of SkyLite Systems, and a MCTS in SharePoint 2007/WSS 3.0, and a CISA (Certified Information Systems Auditor). He is the co-author of *SharePoint Deployment and Governance using COBIT 4.1: A Practical Approach* (www.isaca.org).

Axceler

ControlPoint, the leading governance product for Microsoft® SharePoint™, can help you get your SharePoint ducks in a row. Control your SharePoint ducks as part of a broader governance plan.

Control your

- SharePoint Security
- SharePoint Content
- SharePoint Activity and Storage
- Governance Policies
- And much more

Now that SharePoint 2010 is here, you need a SharePoint governance tool more than ever. So check us out www.axceler.com to learn more.

Microsoft® SharePoint® 2010

Microsoft® GOLD CERTIFIED Partner

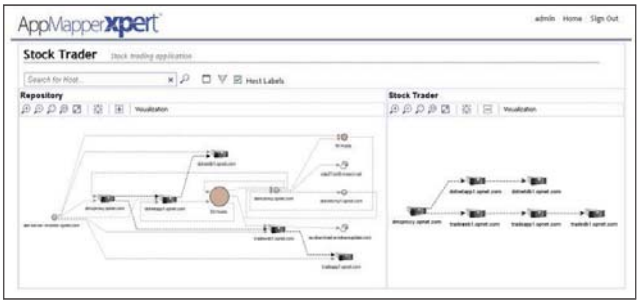
Editors' Best GOLD

Best of tech·ed 2009

Tackle Unstructured Data with Data Insight for Storage

Symantec has announced **Symantec Data Insight for Storage** to help organizations better understand and manage the sharp growth of unstructured data, including files such as documents, spreadsheets, and emails. Data Insight for Storage provides new visibility and control into the ownership and usage of unstructured data to help organizations reduce storage costs and align their information assets to business goals. Capabilities include effective consumption/chargeback to see who is responsible for data; inactive/orphan data organization through owner identification; and better data utilization via reclamation, migration, tiering, and capacity planning. To learn more, visit www.symantec.com.

OPNET Introduces AppMapper Xpert



OPNET Technologies has announced **AppMapper Xpert,** a solution that automatically produces a run-time application map, identifying the underlying application and infrastructure components that enable a production application. AppMapper Xpert will be available through a Software as a Service (SaaS) delivery model, simplifying and accelerating its adoption by IT organizations for all aspects of application management, including performance troubleshooting, planning, virtualization, data center consolidation, and cloud deployment. AppMapper Xpert is part of OPNET's suite of application performance management products. To learn more, visit www.opnet.com.

PRODUCT SPOTLIGHT

Siemon Adds LC Fiber Optic Adapter to LockIT

Siemon has announced the launch of its **LockIT LC optical fiber adapter lock.** This adapter lock protects against unauthorized access to unused LC ports. The adapter locks require no special connectivity and can be utilized to secure nearly any LC optical fiber–based network infrastructure. According to the vendor, the LockIT system is designed to provide physical layer security without adding complexity or impacting overall functionality and density.

The LockIT adapter lock snaps securely into any industry-standard LC port, blocking cord access and preventing tampering. Removable only with a specially designed key, the lock fits flush within the port, providing full access to adjacent ports regardless of density, and it is brightly colored to allow network personnel to quickly identify locked ports. These new secure components are system and cabling performance independent, allowing it to secure any active equipment LC port, or passive LC patching, plug-and-play, or work area port.

"The obvious benefit is a very cost effective and easily implemented deterrent against malicious access to the network through unsecured connectivity," explained Tony Veatch, Siemon director of product management. "But LockIT is also an excellent way to protect against accidental connectivity errors, acting like a 'lock-out/tag-out' system for the network infrastructure. We see great interest in such a solution in public areas including conference rooms, airports, and classrooms. This simple, effective product is suitable for industries such as transportation, finance, retail, hospitality, and education, as well as in mission-critical data center applications."

To learn more about Siemon's LockIT system, visit www.siemon.com/go/lockit.

ATC Releases Updated P2P Marshal, Now with eMule Support

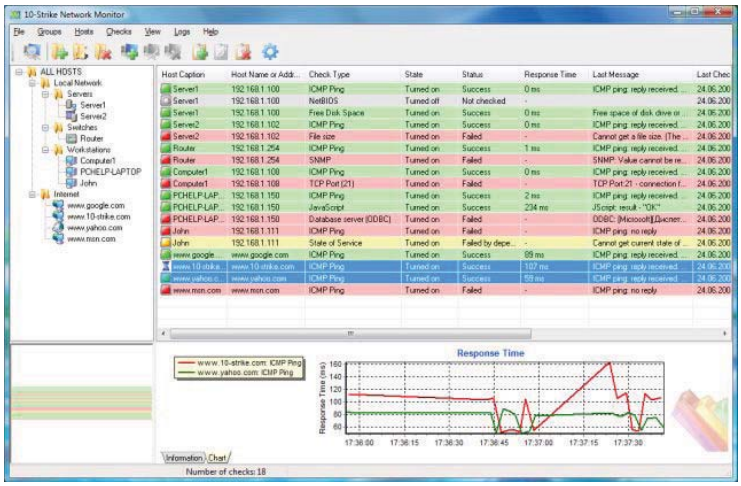
ATC-NY has just released **P2P Marshal 3.1.** P2P Marshal is a computer forensics tool that automatically detects, extracts, and analyzes P2P evidence on hard drives. According to the vendor, a typical data acquisition and analysis that takes hours by hand can run in a few minutes with P2P Marshal. P2P Marshal automatically detects and analyzes peer-to-peer file sharing usage including the most commonly used P2P client programs. The program then presents per-user information on those users in a report. To learn more, visit www.atc-nycorp.com.

Workflow Essentials for SharePoint 2010

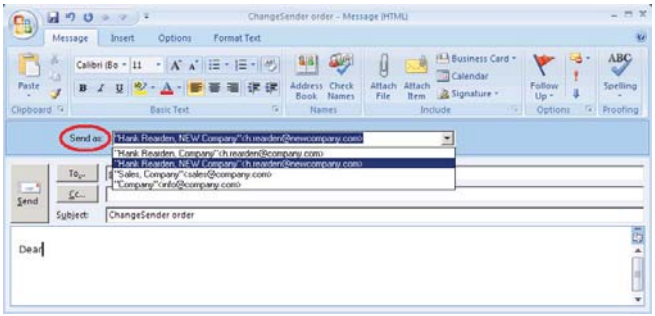
SharePoint Solutions has released **Workflow Essentials for SharePoint 2010,** which enhances and extends SharePoint Workflow options for SharePoint 2010 Server and SharePoint Foundation 2010. This new SharePoint add-on adds 24 new workflow activities and 2 new workflow conditions to those which are available out-of-the-box in SharePoint Designer 2010's workflow designer menu. New workflow activities include "loop through list items," "start another workflow," "create a SharePoint site," and others. To learn more, visit www.sharepointsolutions.com.

Track Local and Internet Traffic Usage

10-Strike Software has announced **10-Strike Bandwidth Monitor 2.0,** a traffic



usage and network bandwidth monitoring tool. The program collects the inbound and outbound network traffic usage statistics on network computers, switches, and other network devices to help an administrator find out which computer utilizes the most of the network bandwidth due to employee abuse, viruses, or another cause. To collect the data, the product supports SNMP, WMI, and via remote agents for Windows machines. The primary change in the latest release is the addition of a packet sniffer. To learn more, visit www.10-strike.com.



Customize Your Email Sender Address Under Outlook and Exchange Server

Servolutions has released **ChangeSender,** a program that works with Microsoft Outlook and Exchange Server to let you choose the address that your emails are sent from on an email-by-email basis. ChangeSender makes it simple to send emails from any valid address. For each email that you send, simply use the Send As selection box, and choose the sender address that you prefer. ChangeSender is even more convenient to use when you're replying to an email. The software can automatically select the recipient address from the incoming email, and use it as your sender address. The program also lets you share email addresses across your company. To learn more, visit www.servolutions.com.

LogLogic 5 Adds VMware vCloud Director Support

VAD Wick Hill announces **LogLogic 5,** with support for the newly launched VMware vCloud Director. LogLogic 5 will provide insight by centralizing and structuring virtual machine operational information, such as log data. The solution shows how the VMware vCloud Director systems are configured, how they react under load, and how they are being used by the customers. The solution will alert data center personnel in real time to operational issues. The alerts will be backed up with forensic discovery tools and all the evidentiary reporting needed. To learn more about the product, visit www.loglogic.com.

Paul's Picks

www.winsupersite.com

SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Web Apps on Windows: IE 9 vs. Chrome

IE 9 PROS: Deep integration with Windows 7, more powerful features

IE 9 CONS: Requires Windows 7, advanced features are hard to discover and won't be widely used

RATING (IE): ◆◆◆◇◇

CHROME 9 PROS: Lack of browser chrome—borders, frames, menus, and toolbars—makes web apps look like apps; automatically makes shortcuts; works with Windows XP and Vista

CHROME 9 CONS: No real OS integration

RATING (CHROME): ◆◆◆◆◇

RECOMMENDATION: Both Internet Explorer 9 (currently available in prerelease form) and Google Chrome integrate web apps into Windows so that they can run side-by-side with native applications, providing a customized browser UI (IE 9) or no browser UI at all (Chrome). IE 9 provides deeper integration with Windows 7 features but requires that OS. Chrome works on XP and Vista, creates a more seamless look, but offers no real OS integration. Try them both and mix and match if required.

CONTACT: Microsoft • www.microsoft.com; Google • www.google.com

DISCUSSION: http://bit.ly/gys3tl

Mac App Store

PROS: Integrated with the OS, liberal reinstallation rights on unlimited Macs

CONS: Limited selection, no big names (Adobe, Microsoft) on board yet

RATING: ◆◆◆◆◇

RECOMMENDATION: Apple's Mac App Store applies the principles, look, and feel of the iPhone, iPod touch, and iPad App Store to the Mac. Even if Windows users get such a thing in Windows 8—if the rumors are correct—Mac users get it now, and it's well done. Apps are easy to download, purchase, install, and update. No big-name players are on board yet—Adobe and Microsoft are holdouts. This is software done right, delivered on an aggressive schedule. In the Windows world, we're not that lucky.

CONTACT: Apple • www.apple.com

DISCUSSION: http: http://bit.ly/gMFAal

InstantDoc ID 129565

REVIEW

PowerBroker Desktops

Most systems administrators subscribe to the principle of granting users as few privileges as possible. However, using standard Active Directory (AD) group policies makes it difficult to give users the privileges to install, run, and configure company-required applications without either granting administrator rights or overly involving the Help desk in assisting users.

BeyondTrust Software's **PowerBroker Desktops** helps ease the burden of implementing the least-privilege desktop for Windows Server 2008 and Windows Server 2003 domains. To get started, I cracked opened the well written and detailed installation guide, which lays out a two-step installation process.

The first step is to install the Beyond Trust Group Policy snap-in on any 32-bit or 64-bit machine that is used to manage Group Policy Objects (GPOs)—a simple and straightforward process. The second step is to deploy the client software via the standard Group Policy software push. This step was problem-free, but because the client is a standard MSI file, any deployment tool can be used.

After I deployed the client and installed the Group Policy snap-in, I was ready to begin defining policies. Creating policies is an intuitive process—you simply open a new or existing GPO that targets the users or machines to manage, right-click the PowerBroker Desktops selection in the GPO, and select *Create new policy.* Policy options include permission escalation (usually Administrator) and privilege (e.g., shut down the computer, act as part of the OS), as well as other optional items. As Figure 1 shows, the policies are broken down into 10 types that let you define exceptions for almost any privilege escalation.

From previous experience with Microsoft Customer Service and Support, I knew that a standard Windows 7 user can't install a printer driver from a Windows-based print server unless seven or more Group Policy exceptions are created. To determine the type of BeyondTrust rule, I attempted to add the printer from the client PC and noticed, through BeyondTrust's handy policy monitor tool (polmon.exe), that ntprint.exe needed a privilege escalation. On the Group Policy management machine, I created a new BeyondTrust path rule (which escalates a program in a defined program file path) that specified the path to ntprint.exe, granted administrator permissions via the Permissions tab, and granted the *Load and unload device drivers* privilege via the Privileges tab. After a Group Policy refresh on the client PC using Gpudate /force, I was able to add the printer.

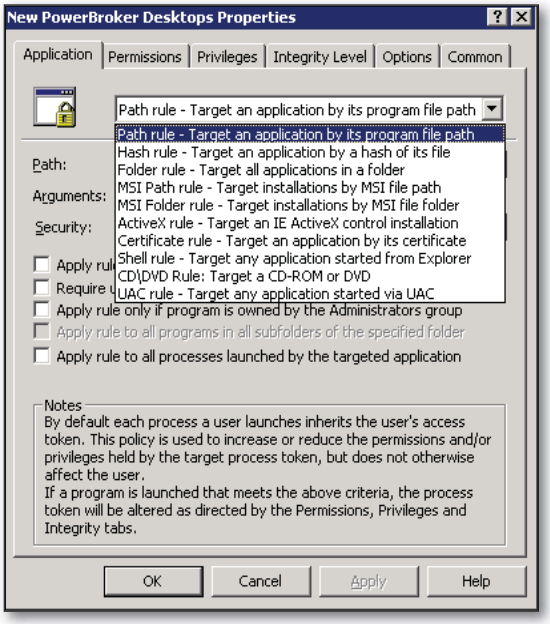


Figure 1: Defining policies

Next, I tested another challenging application as a Windows 7 standard user—GoToMeeting, the web conferencing and online meeting software. The installer is downloaded via an ActiveX control that spawns several .exe file downloads and installation processes. After a few failed attempts, I tried defining an ActiveX and hash exception (which escalates a file permission regardless of where it's executed) for all GoToMeeting .exe files, but the installation still failed. Finally, after consulting with BeyondTrust, I got the installation to succeed by removing the previous rules and using a single shell rule that let me define a program path for exception with arguments. The rule for the Internet Explorer (IE) .exe file grants administrator permissions and all privileges for the GoToMeeting.com sites and subsites. When you use the shell rule with IE, a separate browser session launches on the client; the specified site downloads, and installations run with elevated permissions.

PowerBroker also features some default path rules that solve many common escalation requests that are specific to each Windows version, such as disk defragmentation and adding hardware. Another useful rule type is a folder rule that lets an administrator create a common installation share for users.

I'm impressed with PowerBroker. The product works as advertised and lets administrators create the flexible rules necessary to maintain a desktop with only approved applications and settings. Despite its high cost, PowerBroker would particularly benefit any admin who hasn't rolled out Windows 7 and needs to implement systems that don't have local users in the administrators group.

InstantDoc ID 129362

PowerBroker Desktops

PROS: Simple installation; wide range of rule types; excellent documentation; seamless Group Policy integration

CONS: Licensing cost

RATING: ◆◆◆◆◆

PRICE: Starts at $30 per seat

RECOMMENDATION: PowerBroker will benefit any IT pro who uses AD, particularly those who haven't yet rolled out Windows 7 and need to implement systems that don't have local users in the administrators group.

CONTACT: BeyondTrust Software • 800-234-9072 • www.beyondtrust.com

Tony Bieda | tonybieda@yahoo.com

GFI MAX RemoteManagement

GFI MAX RemoteManagement works a bit differently than most of the system monitoring solutions I've looked at in the past. Instead of a server-based application that you install on a system inside your network, GFI MAX RemoteManagement is a hosted solution. With this product, the server doesn't query each monitored node at specified intervals. Rather, each monitored node has a software agent that's configured to report back to the GFI MAX RemoteManagement system with its current statistics, alerts, and a detailed hardware inventory.

Although the product could be used by an internal IT department to keep a handle on minute-by-minute network or system conditions, its main intended use is as a management solution for independent consultants who support several companies. Having a software agent on each computer gives GFI MAX RemoteManagement an advantage in managing a mobile workforce because the software agent can check in with the system from behind firewalls and wherever the computer gains Internet access.

To deploy the product, you log on to the web console, which Figure 1 shows, and create a hierarchy of businesses and business sites. Each site is associated with one business, and each server or workstation is associated with one of the business sites. You add servers or workstations to each of the sites by installing the software agent on each computer in either server or workstation mode. After the software agent is installed, the computer shows up in the GFI MAX RemoteManagement web console. From this console or software agent interface you can create an installation package that can be deployed to other computers through a Group Policy Object (GPO) or other means. Keep in mind that whatever computer this installation package is installed on will show up in the same company hierarchy as the computer it was created from.

During the installation process, the wizard walks you through a process of choosing which Daily Safety Checks will be tested and reported on. The Daily Safety Checks options for software agents in server mode include:

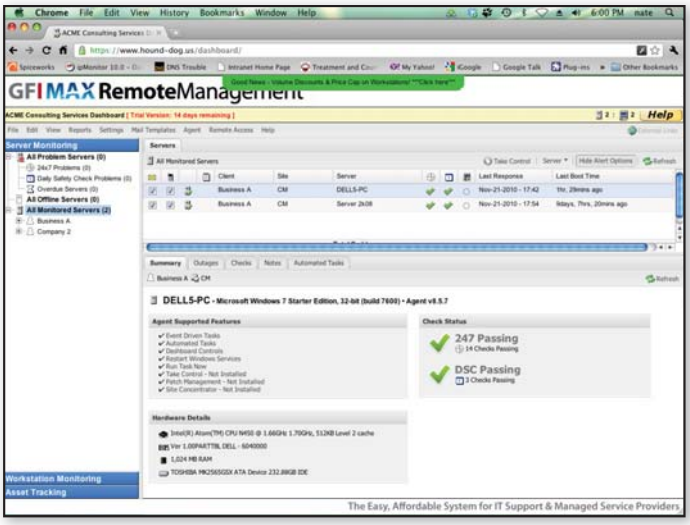


Figure 1: GFI MAX RemoteManagement's web interface

- Antivirus—Checks whether the antivirus software is installed and running the latest updates. (Most major antivirus software packages are supported, but you should check the product's documentation before making a commitment.)
- Backup—Alerts you if a supported backup product fails. (Check product documentation for specific information about supported backup products; currently supported products include those from Acronis, ARCserve, GFI, Microsoft, Symantec, VaultLogix, and Veritas.)
- Drive Consumption (workstation also)—Measures how much disk space is still available.
- Exchange (if applicable)—Verifies that the size of any of your information stores is less than the configured limit.
- WSUS (if applicable)—Checks that the Windows Server Update Services (WSUS) database is updating with its source and identifies the current critical update status of computers on the network.
- File Size (workstation also)—Checks the actual file size; would likely be used if you needed to monitor the size of a database file or database log file. Abnormal growth in a database could indicate a problem or unknown change that should be investigated. Sudden growth in a log file could indicate that a particular process is failing.
- Event Log (workstation also)—These alerts can be configured for the Windows event logs based on event ID, source, type, and text contained in the message area.
- Scripts (workstation also)—You can upload custom scripts from the web console and assign them to individual computers. Supported script types include DOS batch, JavaScript, Perl, PHP, PowerShell, Ruby, Python, and VBScript.
- Critical Events (workstation also)—Similar to the Event Log check in the sense that it looks at the Windows event logs; however, its purpose is to provide a daily report of either the 10 most frequent or 10 most recent events in whichever log you specified when you configured the check.
- Hacker (workstation also)—Number of failed logon attempts.
- Physical Disk (workstation also)—If any of your attached disks is a Self-Monitoring, Analysis, and Reporting Technology (SMART)-type disk and reports errors, GFI MAX RemoteManagement can collect and report these errors.

Nate McAlmond | mcalmond@gmail.com

- SNMPv1/v2c (workstation also)—Allows reporting of any information available via the SNMP protocol. If installed in server mode, the check can be directed at other devices on the network. For example, I had the agent installed on a Windows server in server mode and I was able to receive information about the bandwidth usage of my SonicWALL firewalls. However, when the GFI MAX RemoteManagement software agent is in workstation mode, this check can report only on the local machine's SNMP database.

On the installation wizard's next screen, you can select what the computer will test every 5 or 15 minutes. Some of these checks are the same as the Daily Safety Checks; the difference is that they're checked much more frequently. The 24/7 Checks options for software agents in server mode include:

- Bandwidth Monitoring—Uses SNMP to query network interfaces on the network, such as an Ethernet switch, to identify current throughput and possible performance issues. If a configured threshold is exceeded, an alert can be triggered.
- File Size (workstation also)—Checks the actual file size; would likely be used if you needed to monitor the size of a database file or database log file. Abnormal growth in a database could indicate a problem or unknown change that should be investigated. Sudden growth in a log file could indicate that a particular process is failing.
- Event Log (workstation also)—These alerts can be configured for the Windows event logs based on event ID, source, type, and text contained in the message area.
- Scripts (workstation also)—You can upload custom scripts from the web console and assign them to individual computers. Supported script types include DOS batch, JavaScript, Perl, PHP, PowerShell, Ruby, Python, and VBScript.
- Drive Space (workstation also)—Verifies that the amount of available drive space is greater than the specified minimum.
- Server Performance—Measures processor utilization, processor queue length, memory usage, network interfaces, and physical disk statistics to generate reports and alerts.
- Ping—This check verifies that the monitored machine can still ping other interfaces on the network.
- TCP Service—Checks whether services are still accepting connections correctly, whether the correct ports are open, and whether ports that shouldn't be opened are closed.
- Web Site—Verifies that correct text strings are returned from web servers.
- Windows Service (workstation also)—Verifies that services necessary to the Windows OS are up and running.
- SNMPv1/v2c (workstation also)—Allows reporting of any information available via the SNMP protocol. If installed in server mode, the check can be directed at other devices on the network. If installed in workstation mode, the check can report only on the local machine's SNMP database.

During installation of the software agent, you can select which version (workstation or server) is installed. It doesn't matter which version of Windows is installed on the computer. For the server version of the software agent, you can use the network-based alerts to monitor other devices on the network. The SNMP options include several metrics for major vendors (e.g., Adaptec, APC, Cisco, Dell, HP Compaq, HP Jetdirect, Intel, Linux, NETGEAR, Sonic WALL); in addition, you can manually add the SNMP settings for other devices. If the software agent is installed in server mode, you have much more than just a set of single host check options—you can use a single software agent to look at potentially every addressable device on the network. If the software agent is installed on a workstation, only the local host can be monitored with SNMP. These reports can go out as scheduled status updates or triggered alerts. There's also a mobile version of the GFI MAX RemoteManagement web console that sends a quick run-down of any outstanding alerts directly to your smartphone.

Several reports are available that you can configure the system to automatically send to administrators or customers via email or SMS, as in the case of an independent computer consultant. The report templates can be customized to display the appropriate branding, support numbers, hours of operation, sales promotions, and so on. GFI recommends that you send some type of status update to your customers on a regular basis, not only to show them that they're actually getting something for their monthly payment (typically $1 a day per device), but also to help establish you as the logical point of contact for future problems.

In addition to monitoring, GFI MAX RemoteManagement has the ability to run some basic computer maintenance tasks. From the web console, you can add scheduled tasks to the software agents. These tasks can include defragmenting the disk, clearing the event logs, and clearing the temp files. Tasks can be assigned to the entire site or individual computers. For this reason alone, you might need to set up additional sites to keep server and workstation task management separate. Patch management and remote control are also available, but these features were still in beta at press time.

GFI MAX RemoteManagement is very easy to use and deploy. It's completely reliable and flexible enough for the most distributed of environments. Future console additions include data leak prevention, managed antivirus, mail archive, and mail security. If your company or client is already paying for these features in separate products, GFI MAX RemoteManagement could come in at a very competitive price point. A free trial version of the software is available from GFI Software's website.

InstantDoc ID 129363

GFI MAX RemoteManagement

PROS: Fast, easy, flexible deployment; no large up-front starting costs; intuitive web interface

CONS: Doesn't include a multiple administrator communication mechanism or network map view

RATING: ◆◆◆◆◆

PRICE: Typically less than $1 per day per software agent; contact GFI for details

RECOMMENDATION: This product would be great for anyone working at multiple non-networked locations, such as in a single-company distributed network environment, or in an independent computer consultant capacity.

CONTACT: GFI Software • 888-243-4329 • www.gfi.com

Application Whitelisting Products

Solutions that go above and beyond AppLocker

by Orin Thomas

Application restriction products, or whitelist products, let administrators configure client computers to run only specifically authorized applications. Rather than worrying about users running malware or dangerous scripts, administrators develop a list of authorized applications that users are allowed to run. If an application isn't on the authorized list, the user is simply blocked from running that application. Depending on the complexity of the technology used for whitelisting, these approved applications can be identified by publisher certificate, a hash value "digital fingerprint," or a simple path and filename.

Identification based on publisher certificate is typically the easiest way to manage application whitelisting. When you identify an application based on a publisher certificate, you often have the option of including all future versions of that application in any rule. One drawback of identification on the basis of publisher certificate is that there are still a large number of applications that aren't digitally signed and can't be identified in this manner. Some implementations of this technique only allow whitelisting based on the publisher's name, whereas others allow whitelisting based on the name assigned to the application and the version of that application.

Identification based on hash value lets you generate a digital hash, something like a digital fingerprint, that identifies the target application's executable file. A drawback of digital hashes is that every time the file is modified, through patching or the installation of a new version of the application, the hash value needs to be recalculated because the digital fingerprint has changed. If you're whitelisting based on hash value, you need to come up with a way of keeping your hash values up-to-date as part of your regular patch management cycle.

Identification based on path is the simplest way of identifying files, but it's also the least secure. An advantage of publisher certificates and hash values is that if an executable file is modified by malware, the file will no longer be whitelisted because it will no longer match the identifying properties of the publisher or hash rule. An infected executable file identified by pathname will still be whitelisted because even though the file itself might have become malicious, it will still be identified as safe by the whitelist.

Software Restriction Policies and AppLocker

Windows has had application restriction policies since the release of Windows XP. Software Restriction Policies (SRPs) let you create hash rules and path rules. SRPs have the following benefits and drawbacks:

- They include hash- and location-based file identification.
- They include publisher certificate rules, but they work on an all-or-nothing basis. You either allow all applications signed by a publisher or no applications signed by a publisher. For example, you can't use a publisher certificate rule to allow Adobe Acrobat but block Adobe Photoshop. You need a copy of the publisher's certificate in .cer or .crt format to create an SRP certificate rule.
- They allow you to specify which file extensions indicate that a file is executable.
- They don't include publisher rules.
- Rules must be created manually.
- There's no central reporting solution, other than combing event logs.
- They use native Group Policy functionality; they don't require installation of an extra client.

Windows 7's AppLocker extends the functionality of SRPs. AppLocker offers the following improvements and differences over SRPs:

- You can create a publisher rule based on a sample file rather than needing a separate certificate file in .cer or .crt format.
- You can automatically scan a computer to have a set of publisher and certificate rules created.
- It doesn't support clients other than Windows 7 Professional, Enterprise, or Ultimate editions.
- It must be applied through Group Policy. Lack of client software means administrators must perform substantially more work to get AppLocker working.
- It still doesn't provide a central reporting solution.

If you want to use application whitelisting as part of your organizational security strategy, and you're looking for a product that offers more than SRPs and AppLocker, consider using an application restriction product such as **Lumension Application Control,** Sophos's **Endpoint Security and Data Protection,** or **Bit9 Parity.** All of these products provide substantially more functionality than application whitelisting. Although I mention this functionality, the focus of the following product reviews is to compare their application whitelisting functionality.

Lumension Application Control

Lumension Application Control is a whitelist-specific product that offers automatic application discovery, software update authorization, script and macro protection, application review options, local application authorization, and heuristics to detect malicious code that has been locally authorized on a specific number of computers. Lumension uses hash-based and path-based rules for file identification and lets administrators remotely scan clients to generate file identification lists.

Client deployment. The software ships with both an x64 and an x86 Windows installer in MSI format. Administrators can deploy the software to clients through either Group Policy or more sophisticated solutions such as Microsoft System Center Configuration Manager (SCCM).

Creating and updating policies. Lumension Application Control lets you perform discovery to identify which applications are present in your environment. You use the results of these scans to create application whitelisting policies.

After you identify the files that are present in your environment, you use the Lumension Application Control console to add files to file groups. You use file groups as the basis for blocking or allowing applications. You can apply application whitelists to different users by assigning the users to different file groups. File groups determine which applications are whitelisted for that user, as Figure 1 shows.

Benefits over AppLocker. The biggest benefit over AppLocker is the extensive remote discovery functionality. With AppLocker, you must run the wizard locally on a reference system to create the application list. With Lumension, you simply point the wizard at a target system to generate the list after scanning that system.

Lumension also provides better monitoring functionality with centralized reporting. The product leverages the power of SQL Server databases in generating reports.

Finally, Lumension offers spread check functionality. It automatically blocks the spread of suspicious executable files.

Additional notes. Lumension has a very involved installation process. Whereas the installation for both Endpoint Security and Data Protection and Bit9 Parity is primarily a short wizard that you can easily click through, Lumension Application Control installation involves closely following several pages of detailed instructions. A competent administrator won't find this task to be problematic, but the more complex an installation process is, the more likely an administrator is to make mistakes when implementing it.

Although Lumension Application Control provides a quick and easy way of generating file identification data for use in whitelists, the product documentation suggests using path rules for applications that are regularly updated. As I mentioned earlier, path rules can be problematic from a security perspective because a path rule will still allow an executable file infected by malware to run whereas a certificate rule or hash rule will not.

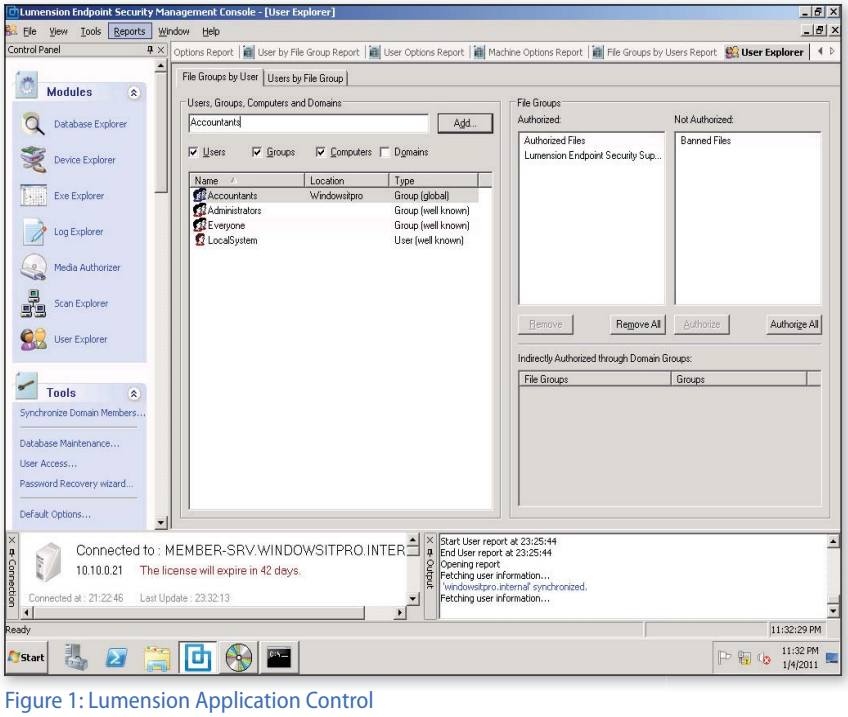


Figure 1: Lumension Application Control

Lumension Application Control

PROS: Straightforward detection of applications; whitelists are easy to create

CONS: Complicated installation routine; difficult to configure

RATING: ◆◆◆◆◇

PRICE: $45 license; $9 per year maintenance

RECOMMENDATION: Admins who are looking for more functionality than AppLocker provides might like this product; however, it has an unnecessarily complicated installation routine.

CONTACT: Lumension Security • 888-970-1025 • www.lumension.com

Endpoint Security and Data Protection 9.5

Sophos's Endpoint Security and Data Protection 9.5 is an advanced endpoint security solution that includes antivirus, firewall, application control, device control, data loss prevention, encryption, and network access control (NAC) functionality for Windows, Linux, Mac, and UNIX clients. As is the case with Bit9 Parity and Lumension Application Control, Endpoint Security uses a SQL Server 2008 Express back end to store application information.

Client deployment. Bit9 and Lumension include standalone client installers, but Sophos uses a push-based installer to push the client from the console to the computer that will be protected. You can download a client file directly from Sophos, but this file isn't included by default.

Administrators have to prepare client computers before attempting to deploy the client from the Sophos console. This process involves modifying the default network and sharing settings, changing the Remote Registry service's startup status, modifying User Account Control (UAC) settings, and modifying the firewall settings.

Creating and updating policies. Sophos application restriction policies

are created by selecting the Application Control node under Policies in the main console. You can create a new policy or edit the default policy. You apply policies to computer groups; a computer can belong to only one custom group at a time.

Sophos provides you with an extensive list of applications, sorted by functionality. The administrator creates a policy by going through the list and determining which applications to allow and which applications to deny. Sophos updates the list on a regular basis, which means that after you allow a specific application, all future iterations of that application will theoretically be identified by Sophos and that identification will pass back down to your endpoint installation. Sophos also continuously adds new applications to its list. It's not directly clear how Sophos deals with custom applications.

The default policy authorizes all applications, although it's relatively simple to block all applications and then add the applications used in your environment to the whitelist. Figure 2 shows an archive tool added to the whitelist. There appears to be no tool included in the product to automatically test which applications are installed on a computer—so unless you have an up-to-date software inventory, you should proceed with caution when building your application whitelist.

Sophos's application control policies are applied on the basis of computer group. You can import existing computer groups from Active Directory (AD) or create your own group hierarchy. Computer accounts can be imported from AD or by scanning the network. Only one application control policy can apply to a group, although the same application control policy can apply to multiple groups.

I was unable to determine from the Sophos documentation or interface how to create whitelist rules for products that aren't included in Sophos's list of identified products. It's unclear if Sophos uses a certificate-based, hash-based, or path-based file identification mechanism. To a certain extent, this is a moot point because the main benefit of using a certificate-based identification mechanism over a hash-based mechanism is ensuring that rules remain up-to-date after applications are patched. Because rule definitions are downloaded through regular updates from Sophos, this isn't a problem.

Monitoring. A specific console lets you monitor all application control–related events. This tool lets you view application control events that occurred within a specific time period, occurred to a specific user, involved a specific computer, or involved a specific application type.

Benefits over AppLocker. Endpoint Security has several benefits over AppLocker. First, Endpoint Security creates identification heuristics for specific applications, so administrators don't have to create them manually. In addition, Endpoint Security updates the application identification database. A drawback of the product is that it doesn't appear to be possible to block a specific version of an application (e.g., Adobe Acrobat 9) but allow a later version of the same application.

Additional notes. Before deploying Endpoint Security and Data Protection, an administrator will need to apply policies to ensure that the appropriate settings are in place and services are started. Without an MSI installer, deployment occurs through the Sophos console. Some administrators might find that using the console for client deployment doesn't scale well for their organizations. But if you're in a heterogeneous environment, Sophos includes support for Mac, UNIX, and Linux clients as well as support for all Windows client OSs.

Handing off rule creation to the vendor has both benefits and drawbacks. The drawback is that it might be difficult to integrate custom executable applications into your rules. The benefit is that by letting Sophos handle rule updates, after you whitelist an application you don't need to worry about maintaining rules for that application.

Endpoint Security and Data Protection 9.5

PROS: Automatic rule maintenance reduces the amount of time administrators have to spend updating whitelist rules; supports Mac, Windows, and Linux platforms

CONS: Unclear how to add either custom software or software not in Sophos's existing list

RATING: ◆◆◆◇◇

PRICE: $11 per user per year for up to 99 users

RECOMMENDATION: This product is part of a broader security suite and might suit organizations with a heterogeneous client deployment of off-the-shelf rather than custom software.

CONTACT: Sophos • 888-767-4679 • www.sophos.com

Bit9 Parity

In addition to offering application whitelisting functionality, Bit9 Parity also offers registry protection functionality, configuration monitoring and drift management, and file inventory functionality.

Client deployment. Bit9 Parity's client deployment is through MSI files that can be deployed either traditionally via Group Policy or with an application deployment tool such as SCCM 2007 R3. Users can also

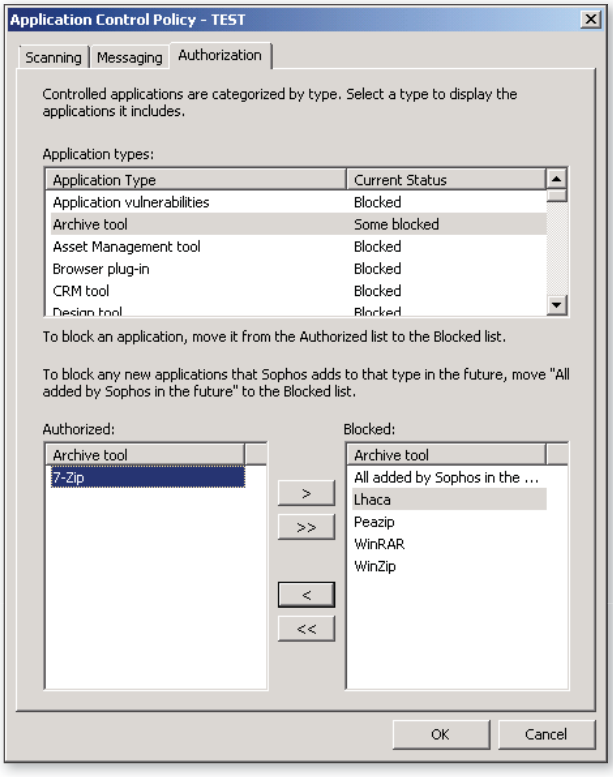


Figure 2: Endpoint Security and Data Protection

install the Bit9 client software directly from file shares on the management server.

Creating and updating policies. Bit9 Parity uses policies to organize computers into groups with similar security requirements. The client software blocks and allows executable files based on settings within the policy. When you create a policy, you configure options for how to deal with approved and unapproved executables, including blocking unanalyzed or unapproved scripts and executables and blocking specific filenames and hashes. Figure 3 shows a Bit9 Parity policy.

You can subscribe to a database hosted by Bit9 that automatically updates your whitelist so that users can run applications that are proven to be safe. Applications that are shown to be unsafe or problematic are automatically blocked.

Monitoring. Bit9 Parity offers monitoring and automatic detection of new applications, as well as administrator notification. This feature lets administrators quickly determine whether any new applications have entered the environment and decide whether to authorize those applications. Unknown applications are blocked by default. After an administrator reviews an application, he or she can approve it.

Benefits over AppLocker. Bit9 Parity has several benefits over AppLocker. First, the product works on Windows Vista and XP clients. In addition, Bit9 Parity includes an online file identification functionality that ensures that when an application is blocked, you can find more detail about the application, such as whether Bit9 considers the file to be a threat or benign. You can also submit blocked applications to Bit9 for the company to provide a threat assessment. Bit9 Parity has substantially better reporting functionality than AppLocker provides. Finally, Bit9 Parity's web-based monitoring console lets administrators connect to multiple clients without having to install a separate management console.

Additional notes. Bit9 Parity currently requires IPv6 to be disabled on the management server. Although the vast majority of organizations aren't using IPv6 on their internal network, this might be a problem for the small number of organizations that have transitioned to an IPv6 infrastructure.

Bit9 Parity has extensive application control functionality. The only drawback of the product is that the extensive functionality can be challenging to leverage for administrators who are unfamiliar with the interface.

Bit9 Parity

PROS: Extensive feature set

CONS: Interface needs reworking to make it easier to leverage the product's extensive functionality

RATING: ◆◆◆◆◇

PRICE: $39 for a perpetual license

RECOMMENDATION: Administrators who are looking for better functionality than AppLocker provides and who take the time to master Bit9 Parity's way of doing things will find the product to be a highly effective whitelisting solution.

CONTACT: Bit9 • 617-393-7400 • www.bit9.com

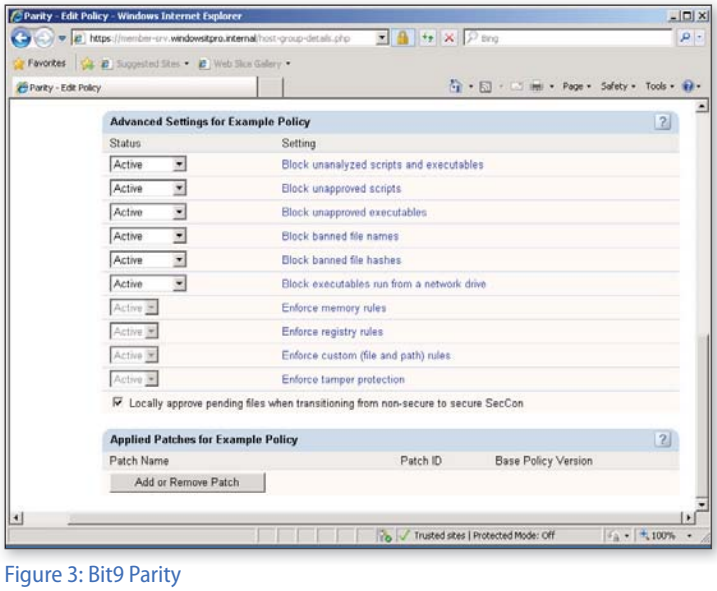


Figure 3: Bit9 Parity

Your Best Bet

Whether you choose to use an application whitelisting product or the native Group Policy functionality depends on your organization's environment and needs. Whitelisting products can substantially reduce the cost of malware infections and unauthorized applications, because an application won't run unless it's on the whitelist. Whitelisting products that go beyond the default functionality that's built into the Windows Server OSs are necessary for most organizations because unless you're running a pure Windows 7 client environment, administrators will spend more time than it's worth to keep SRPs up-to-date.

Maintenance is of critical importance. The biggest cost involved in deploying application whitelisting isn't the products themselves but the amount of time systems administrators will need to spend setting up and maintaining their application whitelists. Bit9 Parity and Lumension Application Control allow for the automatic detection of changed files, giving administrators the ability to quickly adapt to the changing application ecosystem they're responsible for managing. The Sophos approach provides a central list of applications from which whitelists can be generated, but administrators might have questions regarding whether Sophos's list includes all the applications in use at their organization.

It's important to note that the products I reviewed are part of broader endpoint security suites. This review looks at only one specific aspect of these suites rather than attempting to make a comparison across all the features present in each suite. Depending on their taste, administrators might find it easier to accomplish important whitelist maintenance and management tasks using the Bit9 Parity interface than the interface that ships with Lumension Application Control or Sophos's Endpoint Security and Data Protection.

InstantDoc ID 129350

Orin Thomas
(orin@windowsitpro.com) is a contributing editor for *Windows IT Pro* and a Windows Security MVP. He has authored or coauthored more than a dozen books for Microsoft Press.

Enterprise iSCSI SANs

Combine scalable storage with enterprise-class features

by Brian Reinholz

Editor's Note: *Information in this Buyer's Guide is meant to jumpstart, not replace, your own research; also, some products might have been left out, either as an oversight or from lack of vendor response.*

As storage area networks (SANs) have become increasingly affordable, their use in enterprises and even smaller businesses has become widespread. A SAN carries numerous benefits over direct-attached storage. One significant advantage is that all data on SANs is connected via a network—as opposed to direct-attached storage, in which each individual drive is its own separate entity.

The greatest benefit is scalability. Direct-attached storage is limited by the storage capacity of an individual server. Many iSCSI SANs allow for additional nodes, letting some SANs get into the petabytes for storage capacity. If you're trying to justify a hardware purchase for your organization, having a scalable option allows you to propose a solution based on what you need now, without having to worry as much about what needs you may have in one, three, or five years in the future. Finally, as organizations continue to consolidate with more powerful hardware and greater flexibility via virtualization, using a scalable device such as a SAN makes sense.

However, despite the compelling proposition that SANs offer for enterprise storage, iSCSI SANs didn't rise to prominence until a few years ago, with the increased performance of Ethernet networks and reduced costs. Today, iSCSI SANs are an excellent storage choice for most companies, combining the ease of use that simpler storage methods (direct-attached storage) offer with many of the performance and capability gains you'd get with the more expensive Fiber Channel SAN. The biggest drawback to a Fiber Channel SAN is implementation cost and complexity, but Fiber Channel SANs are generally considered to offer faster performance. (Do note, however, that an iSCSI SAN that supports 10GbE might actually be faster than a Fiber Channel SAN.) Other concerns exist as well, such as the limited range of Fiber Channel SANs and the higher maintenance costs.

Some organizations prefer network-attached storage (NAS) over SAN, because a NAS is easier to deploy and generally comes at a lower cost. However, many SANs can also function as a NAS, which offers both ease of deployment and scalability. To learn more about this topic, read "SAN and NAS: Better Together" at www.windowsitpro.com, InstantDoc ID 39189.

Factors to Consider

In the table on the following pages, you'll note the following major distinctions between leading iSCSI SANs. Which product is best for your company will depend on your needs.

Cost. In the table, SAN costs range from a few thousand dollars all the way to $1 million when fully equipped. As with all purchasing decisions, you have to weigh the features most important to your company against budget constraints. (Note, however, that these are list prices and may not reflect the final price a vendor will give you.)

Features. If features such as thin provisioning, replication, and Fiber Channel support are important for your implementation, you'll most likely want to consider one of the higher-end iSCSI SANs. Thin provisioning means greater storage efficiency (don't need unused storage) and replication enhances data collaboration and can simplify data recovery.

Storage capacity. If the features listed above aren't key driving factors, then one of your top priorities will be storage space for your needs. Total capacity ranges across the products in the table from 100TB-3,000TB. Some SANs can also accommodate additional nodes, which increases storage flexibility.

Missing Products

Missing from this Buyer's Guide are several key vendors, including Dell, Oracle, EMC, and IBM. I've tried contacting these vendors but have been unable to obtain information about their products. Also, some vendors aren't included in this Buyer's Guide because their products are low-end SANs, targeted at small businesses. Consider reading last year's iSCSI SAN Buyer's Guide (www.windowsitpro.com, InstantDoc ID 103102) for low-end products under $10,000.

Next Steps

Are you sold on iSCSI SANs? If so, I encourage you to look through the Buyer's Guide table for the product that is best for your needs. If you're not to that point yet, I recommend additional reading, such as "NAS vs. SAN" (www.windowsitpro.com, InstantDoc ID 8692), to help determine the best solution.

InstantDoc ID 129394

Brian Reinholz
(breinholz@windowsitpro.com) is editorial web architect for *Windows IT Pro* and *SQL Server Magazine*, specializing in training and certification.

Company	Product Name	Price	Disk Capacity: Base	Disk Capacity: Total	Speed and Number of Network Interfaces	Fiber Channel Support?	Data Replication Support?	Windows Cluster Shared Volume Support?	Exchange Support?	Can You Add Additional Nodes?
Compellent Technologies 952-294-3300 www.compellent.com	Storage Center	$73,000	6TB of tiered 2.5" 6Gb/ second SAS drives	More than 1,000TB	FCOE, 10Gb iSCSI, 8Gb Fibre Channel, up to 22 total ports in configurable combinations	Yes	Yes	Yes	Yes	Yes, single or dual clustered controllers are available, and up to 77 disk enclosures
D-Link Systems 714-885-6000 800-326-1688 www.dlink.com	DSN-5410-10 with secondary controller	$20,530	12 SAS drive bays (no storage capacity)	168TB (84 SAS drive bays)	80,000 IOPS & 1160MB/sec. - 2x10GbE data ports (1x10GbE ports per controller)	No	No	Yes	Yes	No
	DSN-5210-10 with secondary controller	$17,400	12 SAS drive bays (no storage capacity)	168TB (84 SAS drive bays)	80,000 IOPS & 850MB/sec. - 16x1GbE data ports (8x1GbE ports per controller)	No	No	Yes	Yes	No
	DSN-5110-10 with secondary controller	$12,573	12 SAS drive bays (no storage capacity)	48 SAS drive bays	80,000 IOPS & 425MB/sec. - 8x1GbE data ports (4x1GbE ports per controller)	No	No	Yes	Yes	No
Enhance Technology 562-777-3488 866-537-5140 www.enhance-tech .com	UltraStor ES3160P4-F32TE	$16,695	32TB	128TB	4x GbE iSCSI Ports	No	No	Yes	Yes	No
	UltraStor RS8IP4-F8T	$4,575	8TB	136TB	4x GbE iSCSI Ports	No	No	Yes	Yes	No
	UltraStor RS8IP4-F16T	$5,485	16TB	144TB	4x GbE iSCSI Ports	No	No	Yes	Yes	No
	UltraStor RS16IP4-F16T	$7,190	16TB	144TB	4x GbE iSCSI Ports	No	No	Yes	Yes	No
	UltraStor RS16IP4-F32T	$9,015	32TB	160TB	4x GbE iSCSI Ports	No	No	Yes	Yes	No
	UltraStor RS16IP4-F32TE	$12,533	32TB	160TB	4x GbE iSCSI Ports	No	No	Yes	Yes	No
FalconStor Software 631-777-5188 886-669-3252 www.falconstor.com	FalconStor Network Storage Server (NSS) Gateway Appliance	$22,000	1TB	1,000TB per 2-node cluster	4 x 1Gb Ethernet ports, 2 x 10Gb Ethernet ports, and 2 x 8Gb FC ports	Yes	Yes	Yes	Yes	Yes, 2 nodes; multiple 2-node clusters can be managed together.
	FalconStor Network Storage Server (NSS) HC Series	$40,000	16TB SATA / 3.6TB SAS	896TB	16 x 1GE iSCSI ports or 8 x 1GE iSCSI + 8 x 4Gb FC ports	Yes	Yes	Yes	Yes	Yes, 2 nodes; multiple 2-node clusters can be managed together.
HP 800-282-6672 www.hp.com	P4800 Blade System SAN	$270,000	63TB	504TB	min 8 - max 64 10GbE network ports	No	Yes	Yes	Yes	min 4 nodes, max 32 nodes
	HP 3PAR Storage Systems	$70,000 - $1,000,000+	4.8TB minimum	128TB to 800TB	1Gb/s iSCSI & 0-32 Host Ports	Yes	Yes	Yes	Yes	Yes, up to 8 nodes
NetApp 408-822-6000 www.netapp.com/us/	FAS2000 Series	Contact Vendor	Contact Vendor	104TB	Max FC ports (2, 4, 8Gb): 8; Max Ethernet ports: 1GbE – 8, 10GbE: 4 (FCoE protocol only);Assumes active –active configuration	Yes	Yes	Yes	Yes	No. Only HA pairs are supported
	FAS3200 Series	Contact Vendor	Contact Vendor	1,920TB	Max FC ports (2, 4, 8Gb): 52; Max Ethernet ports: 1GbE – 52, 10GbE – 24;Assumes active –active configuration	Yes	Yes	Yes	Yes	For NAS only, we can scale to 24 nodes or 12 HA pairs. For iSCSI, only HA pairs are supported at this time.
	FAS6200 series	Contact Vendor	Contact Vendor	2,880TB	Max FC ports (2, 4, 8Gb): 96; Max Ethernet ports: 1GbE – 100, 10GbE – 48; Assumes active –active configuration	Yes	Yes	Yes	Yes	For iSCSI, only HA pairs are supported at this time.
QSAN Technology 886-2-7720-2118 ext107 www.qsantechnology .com	P500Q-D424 10GbE iSCSI-SAS 4U24 High Availability Systems	$11,000	24 drives at 48TB	72 drives at 144TB	4 ports 10GbE iSCSI	No	Yes	No	Yes	Yes

	Asynchronous and Synchronous Replication?	Geographical Replication (Across Sites)?	Data Snapshot Support?	Volume Shadow Copy Service (VSS) Support?	Management Software?	Data Protection Manager Software Support?	Remote Management Capability?	Hot-Swap Capability for Drives and Power Supplies?	Fault-Tolerance/ Redundancy Support?	Support for SATA/ SAS/ Both?	Thin Provisioning?	Storage Pool?	Network Interface Teaming for Speed? Redundancy? Both?
	Both	Yes	Yes	Yes	Yes	Yes	Yes	Both	Yes	Both	Yes	Yes	Neither
	Neither	No	No	Yes	Yes	Yes	Yes	Both	Yes	SAS	No	Yes	Both
	Neither	No	No	Yes	Yes	Yes	Yes	Both	Yes	SAS	No	Yes	Both
	Neither	No	No	Yes	Yes	Yes	Yes	Both	Yes	SAS	No	Yes	Both
	Neither	No	Yes	Yes	No	No	Yes	Both	Yes	Both	No	No	Both
	Neither	No	Yes	No	No	No	Yes	Both	Yes	Both	No	No	Both
	Neither	No	Yes	No	No	No	Yes	Both	Yes	Both	No	No	Both
	Neither	No	Yes	No	No	No	Yes	Both	Yes	Both	No	No	Both
	Neither	No	Yes	No	No	No	Yes	Both	Yes	Both	No	No	Both
	Neither	No	Yes	No	No	No	Yes	Both	Yes	Both	No	No	Both
	Both	Yes	Yes	Yes	Yes	Yes	Yes	Both	Yes	Both	Yes	Yes	Both
	Both	Yes	Yes	Yes	Yes	Yes	Yes	Both	Yes	Both	Yes	Yes	Both
	Both	Yes	Yes	Yes	Yes	Yes	Yes	Both	Yes	SAS	Yes	Yes	Both
	Asynchronous	Yes	Yes	Yes	Yes	Yes	Yes	Neither	Yes	SATA	Yes	No	Neither
	Both	Yes	Yes	Yes	Yes	Yes	Yes	Both	Yes	Both	Yes	Yes	Both
	Both	Yes	Yes	Yes	Yes	Yes	Yes	Both	Yes	Both	Yes	yes	Both
	Both	Yes	Yes	Yes	Yes	Yes	Yes	Both	Yes	Both	Yes	Yes	Both
	Asynchronous	Yes	Yes	Yes	Yes	Yes	Yes	Both	Yes	Both	No	Yes	Both

INSIGHTS FROM THE INDUSTRY

SMBs Not Prepared For Disasters, Don't Act Until It's Too Late

Symantec has announced the findings of its 2011 SMB Disaster Preparedness Survey, which measured the attitudes and practices of small- to medium-sized businesses (SMBs) and their customers toward disaster preparedness. The survey findings show that though SMBs are at risk, they're still not making disaster preparedness a priority until they experience a disaster or data loss. The data also reveals that the cost of not being prepared is high, putting SMBs at risk of going out of business. According to the survey, downtime not only costs SMBs thousands of dollars, it also causes customers to leave.

SMBs Still Not Prepared

The findings show that many SMBs do not understand the importance of disaster preparedness. Half of the respondents do not have a plan in place. Forty-one percent said that it never occurred to them to put together a plan, and 40 percent stated that disaster preparedness is not a priority for them.

This lack of preparation is surprising given how many SMBs are at risk. Sixty-five percent of respondents live in regions susceptible to natural disasters. In the past 12 months, the typical SMB experienced 6 computer outages, with the leading causes being cyber attacks, power outages or natural disasters.

The survey revealed that the information that drives most SMBs is simply not protected. Less than half of SMBs back up their data weekly or more frequently and only 23 percent back up daily. Respondents also reported that a disaster would cause information loss. In fact, 44 percent of SMBs said they would lose at least 40 percent of their data in a disaster.

According to the survey findings, half of the SMBs that have implemented disaster preparedness plans did so after experiencing an outage and/or data loss. Fifty-two percent put together their plans within the last six months. However, only 28 percent have actually tested their recovery plans, which is a critical component of actually being prepared for a potential disaster.

Lack of Preparedness Impacts the Business

Disasters can have a significant financial impact on SMBs. The median cost of downtime for an SMB is $12,500 per day. Outages cause customers to leave—54 percent of SMB customer respondents reported they have switched SMB vendors due to unreliable computing systems, a 12 percent increase compared with last year's survey. This downtime can also put them out of business. Also, 44 percent of SMB customers surveyed stated that their SMB vendors have temporarily shut down due to a disaster.

Customers of SMBs also reported considerable effects to their own businesses. When SMBs experience downtime, it costs their customers an average of $10,000 per day. In addition to direct financial costs, 29 percent of the customers surveyed lost "some" or "a lot" of important data as a result of disasters impacting their SMB vendors.

The survey found that 36 percent of SMBs intend to create a disaster preparedness plan in the future. As these and other organizations create plans, Symantec offers the following recommendations:

- ***Don't wait until it's too late:*** It is critical for SMBs to not wait until after a disaster to think about what they should have done to protect their information. Not only is downtime costly from a financial perspective, but it could mean the complete demise of the business. Begin mapping out a disaster preparedness plan today. A plan should include identification of key systems and data that is intrinsic to the running of the business. Basically, identify your critical resources.
- ***Protect information completely:*** To reduce the risk of losing critical business information, SMBs must implement the appropriate security and backup solutions to archive important files, such as customer records and financial information. Natural disasters, power outages, and cyber attacks can all result in data and financial loss, so SMBs need to make sure important files are saved not only on an external hard drive and/or company network, but in a safe, off-site location.
- ***Get employees involved:*** SMB employees play a key role in helping to prevent downtime, and should be educated on computer security best practices and what to do if information is accidentally deleted or cannot easily be found in their files.
- ***Test frequently:*** After a disaster hits is the worst time to learn that critical files were not backed up as planned. Regular disaster recovery testing is invaluable. Test your plan anytime anything changes in your environment.
- ***Review your plan:*** If frequent testing is not feasible due to resources and bandwidth, SMBs should at least review their disaster preparedness plan on a quarterly basis.

Symantec's SMB Disaster Preparedness Survey is the result of research conducted in October and November 2010 by Applied Research, which surveyed IT professionals responsible for computers, networks and technology resources at SMBs.

—Jason Bovberg

1&1® WEB HOSTING

PROFESSIONAL WEBSITES

As the world's largest web host, we know the developer features you need in a hosting package!

.com .info .org .net

Domains Included
All hosting packages include domains, free for the life of your package.

Unlimited Traffic
Unlimited traffic to all websites in your 1&1 hosting package.

Developer Features
Extensive language support with PHP 5/6 (beta) with Zend Framework and git version management software.

Online Marketing Tools
SEO tools to optimize your website.
1&1 Webstatistics makes it easy to monitor your progress.

Green Data Centers
We're committed to hosting your site with a minimal impact on the environment.

1&1® HOSTING PACKAGES
6 MONTHS FREE!*
OFFER EXTENDED!

1&1® BUSINESS PACKAGE:

- 3 Included Domains
- Private Domain Registration
- 250 GB Web Space
- UNLIMITED Traffic
- NEW: Version Management Software (git)
- 2,500 E-mail Accounts
- 50 MySQL Database (100 MB)
- 25 FTP Accounts
- E-mail Marketing Tool
- 24/7 Toll-free Customer Support

~~$9.99~~ per month*

Need more domains?
.info domain only $0.99 first year*
.com domain only $4.99 first year*

More special offers available on our website!

1&1®

MEMBER OF united internet

Get started today, call 1-877-GO-1AND1 **www.1and1.com**

*Offers for a limited time only. 12 month minimum contract term applies for web hosting offers. Setup fee and other terms and conditions may apply. Domain offers valid first year only. After first year, standard pricing applies. Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet AG, all other trademarks are the property of their respective owners.

Why the iPad has a Place in the Enterprise

When Apple first brought the iPad to market, some critics lampooned it as a product without an audience, or an answer to a question nobody asked. Robust sales and a surprising level of penetration in the enterprise have laid most of these concerns to rest, and, if CES 2011 was any indication, Apple will soon face an army of tablet competitors from dozens of other vendors. Some—like the Motorola Xoom and RIM PlayBook—may finally give the iPad the competition it needs.

So why has the iPad succeeded where others have failed? And what do tablets offer that other computing devices don't? Here are a few reasons why I think the tablet form factor may finally have found its niche in corporate America.

Sometimes enough is enough. I'll be the first to admit that my laptop preferences tend to drift toward the overpowered. I really don't need a laptop to have a monster processor, powerful graphics card, vast amounts of storage, Wi-Fi, Bluetooth, and a video camera to write articles. But, having that capability when I might need it is smart, right? People predisposed to having the most powerful laptops aside, the vast majority of office workers probably don't need (or care) if their laptops sport the latest bells and whistles, as long as they let them get on the corporate network, browse the web, view documents and presentations, and check their Facebook pages now and then. The iPad excels at all of these things. It won't replace a desktop or laptop for content creation, but it excels as a device that displays and presents information. And sometimes that's all you need.

Collaboration is king. Have you ever tried to share information on a laptop with 4–5 people seated around a small table? There's lots of laptop turning involved, adjusting the screen for glare, standing up to get a better view of the screen, and peering around the plastic barrier of the laptop screen to make eye contact with the person behind it. The iPad excels as a tool for small, collaborative groups. The device can be easily passed around to participants, or everyone can peer down at the device as it rests in the center of the table. That ability for people to easily share and view the device also makes the iPad ideal for playing digital versions of such popular board games such as Risk, Scrabble, and Monopoly.

Instant information. Like the iPhone, the iPad has a start-up time measured in seconds. We've all been in meetings where everyone patiently waits for someone to pull their laptop out of its case, turn it on, wait for it to boot, and then navigate to the information required for the meeting. Fast start-up time is a boon for sales people, who now have even more time to present information and pitch prospective clients. On the productivity front, how many hours (through the course of a year) have we all wasted waiting for someone's PC to boot? The main reasons people bring laptops to meetings is to provide information relevant to the topic at hand, present documents, share a slide deck, or search the web. The iPad can also connect to a projector for bigger meetings.

Simplicity trumps complexity. I'll admit that I couldn't live without my work laptop. I'm a writer and editor by trade, so the thought of typing a 3,000-word article on a touch screen would be torture. But I also admit that laptops have their own share of drawbacks. They tend to be heavier and more cumbersome, and lugging them between conference rooms can be a chore. Start-up times are longer, and how many of us have had problems with waking up a laptop from sleep or hibernate mode? And how many meetings have we all been in where we watch someone try in vain to get his/her $2,000 laptop to work with a $4,000 projector?

The iPad solves most of these problems: it's light, slips easily on top of notepads and binders, and starts up instantly. The iPad's greatest strength is its intuitive operation and simplicity—traits which are often more valuable than the faster processor speed and more voluminous storage capacity offered by an overly-complex (and expensive) laptop.

I'm sure there are other reasons why people are using the iPad, and I'm sure there's an equally long list of reasons why people aren't using it. If you fall into either camp, shoot an email to jeff.james@penton.com or tweet @jeffjames3.

—Jeff James

AD INDEX

For detailed information about products in this issue of *Windows IT Pro*, visit the web sites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

- *asp.netNOW*
- *DevProConnections UPDATE*
- *Exchange & Outlook UPDATE*
- *Security UPDATE*
- *SharepointPro Connections UPDATE*
- *SQL Server Magazine UPDATE*
- *Windows IT Pro UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Diane Madzelonka at Diane.madzelonka@penton.com.

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the Web. Includes FREE access to eBooks and archived eLearning events, plus a subscription to either Windows IT Pro or SQL Server Magazine.
www.windowsitpro.com/go/vipsub

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePointPro Connections

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.
www.sharepointproconnections.com

NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Windows IT Pro

by Jason Bovberg

Geek Style

PRODUCT OF THE MONTH

The German company Novero (www.novero.com) boasts one of the snazziest websites we've come across in a long time, and there's no denying that its products are equally snazzy. Offering "finely crafted jewelry combined with hands-free innovation," Novero's products seek to erase the boundary between technology and jewelry—in short, to make Bluetooth beautiful. Check out the website for gorgeous representations of Novero's Les Carats, Pavee Noire, Couronne d'Or, and Pavee d'Or headsets. Just don't be too surprised by the prices, which can reach up into the six digits.

USER MOMENT OF THE MONTH

Like any IT pro, I'm constantly asked to fix computer problems for family and friends, as well as friends of family. A while back, a friend of the family called me to say that her Windows XP machine was acting up. The system was running slow, asking for updates. A program would work one day but not the next, or it would just disappear. So, I dropped by and took a look, asking a few more questions but ultimately scratching my head. I poked around and finally looked at Event Viewer. I noticed a preponderance of system restores, so I asked her about them. Her response? To remove an application, she was using System Restore! She'd find where the application was installed, and roll back to that point.

—Ed

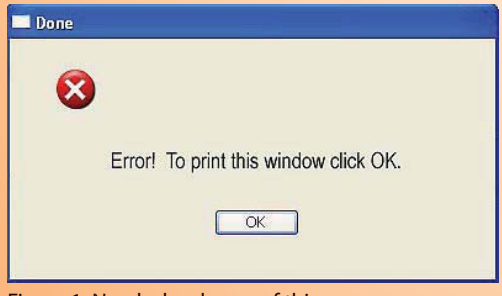


Figure 1: Need a hard copy of this

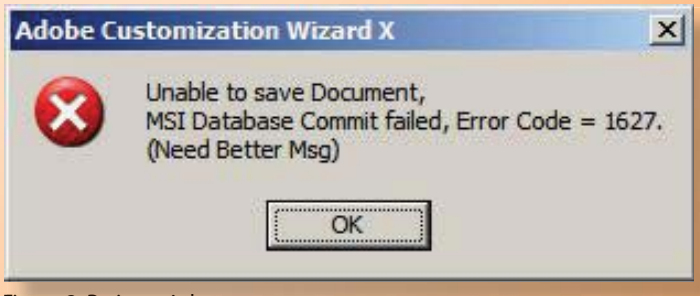
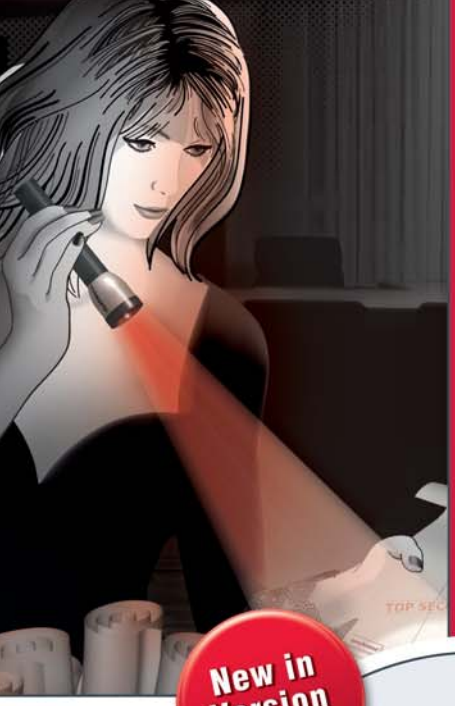


Figure 2: Patience is key

March 2011 issue no. 199, *Windows IT Pro* (ISSN 1552-3136) is published monthly. *Windows IT Pro,* 748 Whalers Way, Fort Collins, CO 80525, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 748 Whalers Way, Fort Collins, CO 80525. Advertising rates furnished upon request. Periodicals Class postage paid at Fort Collins, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,*** 748 Whalers Way, Fort Collins, CO 80525**. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 748 Whalers Way, Fort Collins, CO 80525. Printed in the USA.



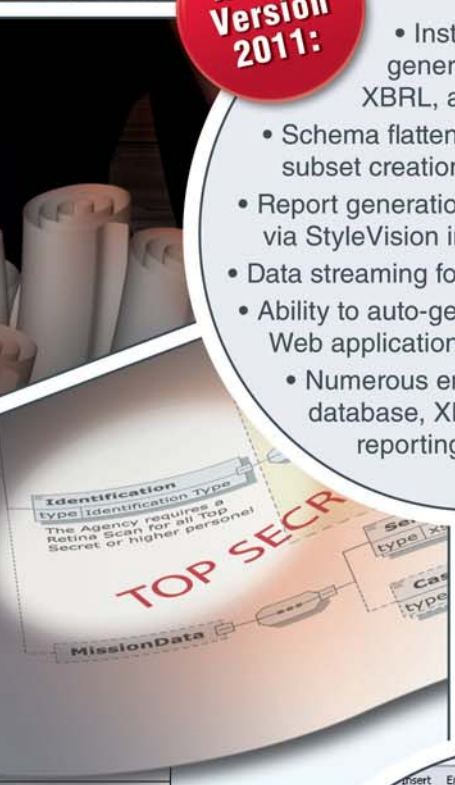
Bring your XML development projects to light with the complete set of tools from Altova®

ALTOVA® missionkit®

Experience how the Altova MissionKit®, the integrated suite of XML, database, and data integration tools, can simplify even the most advanced XML development projects.

New in Version 2011:

- Instant chart generation for XML, XBRL, and databases
- Schema flattener & schema subset creation
- Report generation in MapForce via StyleVision integration
- Data streaming for ETL
- Ability to auto-generate ASPX Web applications
- Numerous enhancements for database, XML, and XBRL reporting



The Altova MissionKit includes multiple intelligent XML tools – now with cutting edge chart and report generation:

XMLSpy® – industry-leading XML editor

- Support for all XML-based technologies
- Graphical editing views, powerful debuggers, code generation, & more

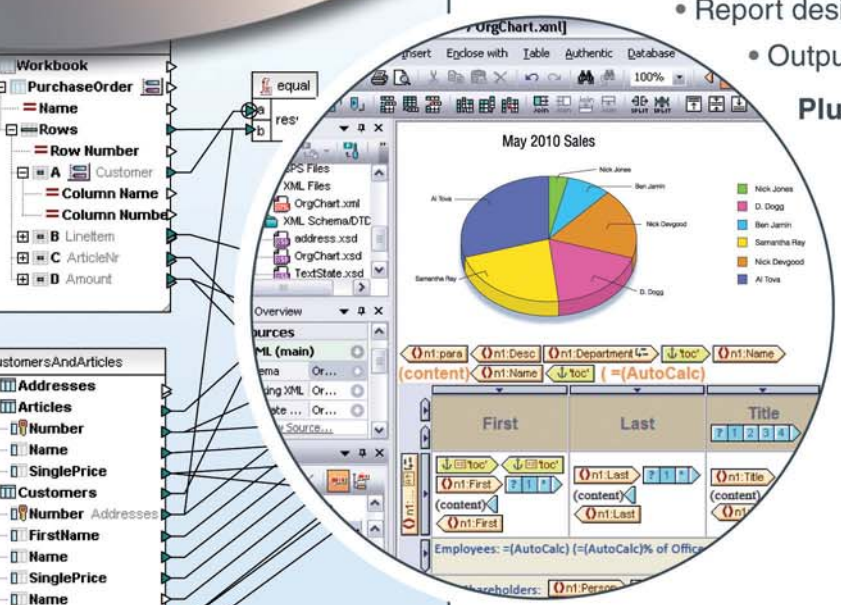
MapForce® – graphical data mapping & ETL tool

- Drag-and-drop data conversion with code generation
- Support for XML, DBs, EDI, Excel® 2007+, XBRL, flat files & Web services

StyleVision® – visual stylesheet & report designer

- Graphical stylesheet and report design for XML, XBRL & databases
- Report designer with chart creation
- Output to HTML, PDF, Word & eForms

Plus up to five additional tools…



Download a 30 day free trial!

Try before you buy with a free, fully functional, trial from **www.altova.com**


* Standard messaging and data charges apply.
Windows Server Hyper-V
I CAN FULLY EMBRACE TOMORROW AT ANY GIVEN MOMENT TODAY.
I HAVE CLOUD POWER.
Only Microsoft gives you a common set of tools that spans the private and public cloud. So you can build your private cloud based on Windows Server Hyper-V today and be ready for a familiar public cloud at a moment's notice. Making the future look a little more like home. That's Cloud Power.
Find yours at Microsoft.com/cloud/privatecloud
Get the free mobile app at http://gettag.mobi or text ITPRO1 to 70700*
Microsoft
Cloud Power